Elcap Firewall For Customer

사용자 설명서

Version 1.1

주식회사 스마일서브

■ 목 차

1. WHY EL CAP?

ELCAP firewall은 2년 동안의 R&D를 통해 ㈜ 스마일 서브에서 직접 개발한 방화벽 시스템입니다.
기존의 상용 방화벽 플랫폼으로는 총 6기가의 트래픽 컨트롤, 2000대의 서버에 맞춤형 방화벽 서비스 제공, 유동IP를 이용하는 대부분 고객들의 네트웍 환경 등을 충족할 수 없는 관계로 2년 여의 개발 과정과 테스트 단계를 거쳐 자신 있게 대 고객 서비스로 선보입니다.
ELCAP 은 미국 캘리포니아 YOSEMITE 국립공원에 있는 EL CAPITAN 이라는 거벽(BIG WALL)의 애칭으로 암벽 등반가 누구나 오르기를 꿈꾸는, 세계에서 가장 난이도 높은 암벽입니다.
섣불리 오르기 힘든 ,누구에게나 든든한 네트웍 서비스 환경 제공을 제공하자는 저희 서비스의 의지를 담아 방화벽 서비스를 ELCAP이라 명명 하였습니다

EL CAPITAN(사진출처: HTTP://YOSEMITE.ORG)

2. ELCAP FIREWALL의 특징

1) 네트웍 상단에 설치되는 H/W 방식의 FIREWALL로 플랫폼에 독립적입니다

고객의 서버에 프로그램을 설치해야 하는 일부 방화벽 프로그램과는 다릅니다.

고객 네트웍 상단에 설치되는 FIREWALL로, 고객 서버가 어떠한 운영 체제를 사용하든 서비스 이용이 가능 합니다.

리눅스 서비스만 설치 가능하고 윈도우 서버는 설치 불가능한 방화벽서비스-일부 서비스 업체에서 리눅스에서 기본 지원되는 IPTABLE에 인터페이스만 올려서 서버에 설치 해주는 것과는 차별화 되어 있습니다.

서버의 운영체제는 방화벽 서비스 이용에 아무런 장애물이 되지 않습니다.

2) 이용이 쉽습니다.

사무실 인터넷 공유기를 설치할 수준이면 됩니다.

방화벽이 뭐에 사용하는 건지 아는 수준이면, 이용 하는데 아무런 어려움 없이 이용 할 수 있습니다.

3) Virtual FIREWALL 서비스(맞춤형 방화벽 서비스)

고객이 직접 컨트롤 하는 웹 인터페이스 기반의 방화벽 제어 화면 제공

일반적으로 시중에 판매 되는 방화벽은 방화벽 관리자가 정책을 세운 후 방화벽을 가동하는 방식으로, 이러한 기존 방화벽 시스템의 문제점은 방화벽 관리자에게 전화나 EMAIL로 방화벽 포트를 열어 달라고 해야 한다는 문제점이 존재 합니다.

ELCAP FIREWALL은 별도의 클라이언트 설치 없이 웹 브라우저가 설치된 컴퓨터면 어느 곳에서나 자신IP에 관한 한 자신의 방화벽 시스템처럼 제어가 가능하여, 원하는 시점에 언제라도 직접 제어가 가능 하여, 마치 자신의 독자 firewall을 운영 하는 것처럼, 서비스 신청 시 생성한 ID로, 자신의 서버의 IP의 포트별 접근 컨트롤을 직접 수행하게 됩니다

4) 배보다 배꼽이 크지 않습니다.

방화벽 서비스 이용료는 몇 만원~ 몇 10만원인데, 방화벽 내부로의 접근 IP 제어 때문에 매월 수 십,수백 만원 하는 고정 IP 전용선을 사용해야 하는 방화벽 서비스와는 질적으로 차별화 되어 있습니다.

고가의 **고정 IP 전용선을 사용하지 않는 중소 규모의 비즈니스 환경에서도 이용이 용이**하도록 설계였습니다.**유동 IP 전용선 이용 고객을 위한 최적의 방화벽 솔류션입니다.**

5) 공유 방화벽 서비스 입니다.

방화벽의 운영은 마치 독자적인 방화벽 시스템을 운영하는 것처럼 보이지만 여러 대 서버가 DMZ를 공유 하는 형태의 방화벽 서비스 입니다.

따라서 방화벽을 공유하고 있는 DMZ 배부의 서버 사이의 침입 시도는 방화벽으로 막을수 없습니다. 여러 대의 서버를 이용하는 코로케이션 고객은 별도의 독자적인 방화벽을 구성할 수 있습니다.

3. 방화벽(FIREWALL)의 이해

네트웍에 연결되어 있는 컴퓨터에는 65,536개의 문(포트)이 있습니다.

서버 프로그램은 약속된 특정 문을 열고 그 문으로 들어 오는 클라이언트의 요구에 대해 어떠한 액션을 취하거나, 반응을 하도록 만들어진 프로그램을 말합니다.

크래킹이란 그러한 문을 열고 있는 프로그램을 공격하여 오 작동하게 만들거나, 속이고 들어와서 컴퓨터의 주인장 행세를 하거나, 아예 컴퓨터를 못쓰게 하는 행위를 말합니다.

서버를 크래킹으로 지키는 방법은 어떠한 면에서 보면 성을 적들의 침략으로부터 성문을 굳게 지키는 행위로 생각하면서 이해하면 ,네트웍 보안에 대해 쉽게 이해 할 수 있습니다.

성을 굳건히 지키기 위해서

1) 적들의 교란 행위에 대하여 병사들을 잘 훈련 시켜서 언제든지 잘 싸울 수 있도록 하고

2) 성의 출입 통제 시스템을 잘 유지하여 적의 스파이가 들어올 수 없도록 하고,

3) 불법적인 침입이 있을 때 이를 즉시 깨닫고 바로 조치 할 수 있도록 하는 것처럼

불법적인 크래킹으로부터 자신의 서버를 안전하게 지켜 내기 위해서

1) 적절한 시스템 보안 패치를 통해 보안 허점이 없도록 포트를 열고 있는 서버 프로그램을 튼튼히 하여, 컴퓨터가 서비스 거부 공격으로부터 루트를 탈취 당하는 일이 없도록 하고

2) 방화벽 시스템을 통해서 열려 있는 포트를 완전히 열거나 ,인가 받은 특정 IP의 클라이언트만 접근을 하거나 불량한 접근자는 아예 출입을 금하는 기능을 하고

3)꾸준한 네트웍 모니터링을 통해서 공격이 의심되는 자의 침입시도가 있을 때 이를 감지하고, 이에 대한 방어 조치를 취하는 행위를 합니다.

따라서 **방화벽의 기능은**

네트웍의 최상단 레이어에 위치하며, 서버의 포트에 대한 나가고 들어 오는 것을 제어하는 수문장의 기능 을 수행하게 됩니다.

다시 말해 대부분의 모든 방화벽의 기능은 특정 IP에서 접근하는 포트에 대해서

1) 누구나 접근을 허용(ANONIMOUS OPEN) 할 것인가?

2) 특정 IP 에 대하여만 접근을 허용 할 것이인가? (MY AREA OPEN)

3) 특정 IP에게는 접근을 완전히 봉쇄 할 것인가? (ALWAYS DROP)

를 결정하는 기능을 기본적으로 가지게 됩니다.

4. ELCAP FIREWALL의 용어 정의

- 일반적으로 아래의 용어를 자주 사용합니다.

용어	용어설명
ACCEPT	패킷을 허용한다는 의미
DROP	패킷을 봉쇄한다는 의미.
OPEN	서버에 열려있는 포트를 의미
서비스	포트 or 서버에서 운영중인 Contents 를 의미
정책	서버에 운영중인 포트에 대한 접근 허용 여부
Elcap 정책	큰 의미의 정책으로 ACCEPT 할 정책과 DROP 할 정책을 그룹으로 모아 놓은 정책을 의미한다. (ANONYMOUS OPEN, MYAREA OPEN, ALWAYS DROP, 특정서버접근, MANAGE IP)

5. ELCAP FIREWALL 기본 내역

1) 기본 설명

일반적인 방화벽은 방화벽 관리자가 정책을 세운 후 방화벽을 운영하는 방식이나,
Elcap Firewall은 고객이 Web 환경을 통해 고객서버의 정책을 직접 세우고,
정책을 적용 시키는 방식입니다.
Elcap Firewall은 Elcap Firewall Web 과 Elcap Firewall 2가지로 구분하고,
Elcap Firewall Web은 고객이 고객서버를 직접 Control 할 수 있는 인터페이스이며,
Elcap Firewall은 방화벽을 의미합니다.

2) Elcap Firewall 정책 설명

1. ANONYMOUS OPEN

A. 모든이가 접근할 수 있는 서비스(포트)를 의미합니다.
Ex) SMTP(25), HTTP(80), POP(110), IMAP(143)

2. MYAREA OPEN

A. 특정한 IP or IP대역 에서만 접근할 수 있는 서비스(포트)를 의미합니다.
Ex) ANONYMOUS OPEN에 입력된 서비스를 제외한 모든 서비스

3. ALWAYS DROP

A. 특정 IP or IP대역 에서는 접근할 수 없게 하는 서비스(포트)를 의미함
B. ANONYMOUS OPEN에 등록되어 있는 서비스(포트)만 입력이 가능하다.
Ex) 특정IP(210.154.145.13)에서 HTTP(80) 에 Attack을 가한다거나,
바이러스 패킷을 보낸다면, 모든 IP에서는 패킷을 ACCEPT 하나,
특정IP(210.154.145.13)를 DROP 시킬 수 있습니다.

4. 특정서버접근

A. 위 3가지 정책 설명은 고객서버가 서버입장에서의 정책이고,
(어떤이가 고객서버로 접근할 때의 정책)
특정서버접근은 고객서버가 클라이언트 입장이 되었을 때의 정책입니다.
(고객서버에서 다른 서버로 접근할 때의 정책)
예를 들어 고객서버에서 다른 FTP서버에 접근할 경우
고객서버에서 다른 HTTP서버에 접근할 경우
고객서버에서 Microsoft 서버에 접속하여 Window Update 할 경우
고객서버에서 다른 서버로 접근할 때 접근하는 서비스(포트)를
등록시켜야 합니다.

일반적으로 Window는
FTP(TCP 20포트 , TCP 21포트, UDP 20포트), SMTP(TCP 25포트),

DNS (TCP 53포트, UDP 53포트), HTTP(TCP 80포트),
인터넷품질테스트(TCP 8020포트,8031포트),
Netbios-ssn(TCP 139포트) – Window directory service
Web-ssl(TCP 443포트), Ms-sql(TCP 1433포트), MSN(TCP 1864포트)

Unix, Linux는 FTP(TCP 20포트 , TCP 21포트, UDP 20포트), TIME(TCP 37포트),
SMTP(TCP 25포트), WHOIS(TCP 43포트), DNS (TCP 53포트, UDP 53포트),
HTTP(TCP 80포트), Web-ssl(TCP 443포트)

를 등록시켜 주어야 고객서버에서 다른서버로 접근을 할 수 있습니다.
특정서버접근 정책은 Elcap 초기화 단계에서 자동적으로 입력이 됩니다.

5. **MANAGE IP**

A. 위 4가지 정책은 포트 기반의 정책이고, MANAGE IP는 아이피 기반의 정책입니다. MANAGE IP에 등록된 IP는 서비스하는 모든 포트에 접근이 가능하게 됩니다.

6. ELCAP FIREWALL 처음 사용자 WORKFLOW

1. 서비스 로그인	http://elcap.100dedi.com
2. 정책 초기화	방화벽 설정함
3. PORT SCAN	IP에 해당 하는 서버의 열려 있는 PORT를 SCAN합니다.(정책초기화에 포함)
4.권장정책 VIEW	열려있는 PORT에 대하여 권장정책을 보여주는 화면 제공.(정책초기화에 포함)
5. 설정 변경	고객이 원하는 포트별 정책을 입력 합니다.(정책초기화에 포함)
6. 저장 및 이용	설정 한 정책의 저장 및 방화벽 서비스 이용.(정책초기화에 포함)

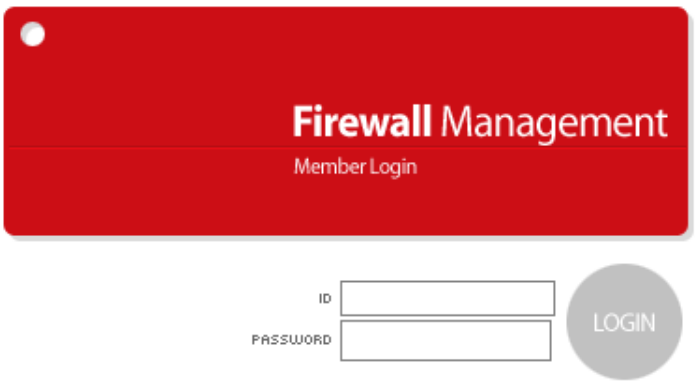
1. http://elcap.100dedi.com에 로그인 합니다.(http://www.100dedi.com 에서 부여된 계정)
2. Elcap 초기화를 실행합니다. (위의 그림 2~6번에 해당 합니다.)
3. Elcap 초기화 만으로 대부분의 크래커들의 공격을 막을 수 있습니다.
4. Elcap Firewall 매뉴얼을 보면서 고객서버에 맞는 정책을 하나씩 하나씩 추가하시면 Elcap Firewall 활용을 아주 잘 하시는 겁니다.

7. ELCAP FIREWALL WEB 인터페이스 안내

주의사항

1) Elcap Firewall Web 은 한명 밖에 Login을 할 수 없습니다.
2) Elcap Firewall Web 에서 작업을 마무리하고 나올 때에는 Logout을 꼭 해야 합니다.
   Logout 하지 아니하고 창을 닫는다면, 2분 동안은 Login 할 수 없습니다.

Login [#그림 1]



설명

- http://www.100dedi.com 에서 부여 받은 계정(id, password)으로 Login을 합니다.
  Login 후 Elcap Firewall을 사용하시면 됩니다.

고객서버 리스트 [#그림 2]

설명

A. Login 을 한 후 보이는 첫 페이지입니다. 고객서버 리스트 페이지 입니다.

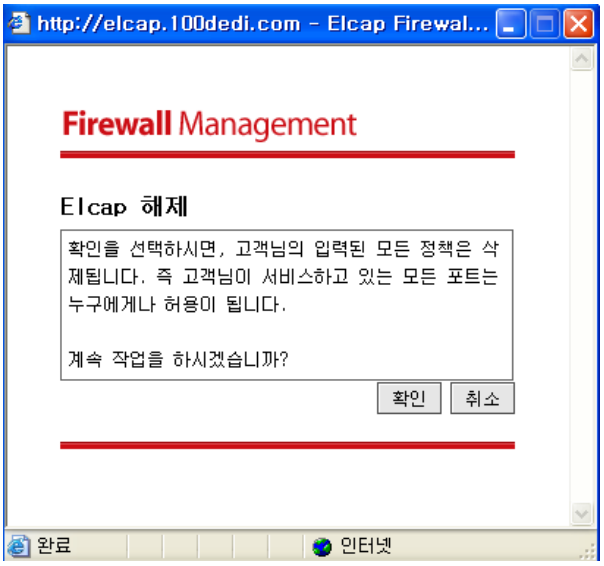
B. 메뉴

1. No - 고객서버 Number 입니다.
2. 서버IP - 고객서버 IP 입니다.
3. Elcap 해제 - 기존에 등록된 정책을 모두 해제(삭제) 합니다.(모든 패킷 허용)
4. Elcap 초기화 - Elcap Firewall을 사용하기 전에 가장 먼저해야 할 사항.
5. Elcap 정책설정 - 수동으로 Elcap Firewall 정책을 설정하는 메뉴입니다.
6. Elcap 정책보기 - 고객이 설정한 정책을 보여주는 메뉴입니다.
7. 서버PortScan - 고객서버를 PortScan 한다.
8. 서버 PortList - 각각의 운영체제 별로 PortScan 할 PortList를 보여주는 메뉴입니다.
9. OS - 고객서버의 운영체제 입니다. (Unix Linux 계열, Window 계열, 스위치 계열 3가지가 있습니다.

서버IP

- 고객서버 IP 입니다.

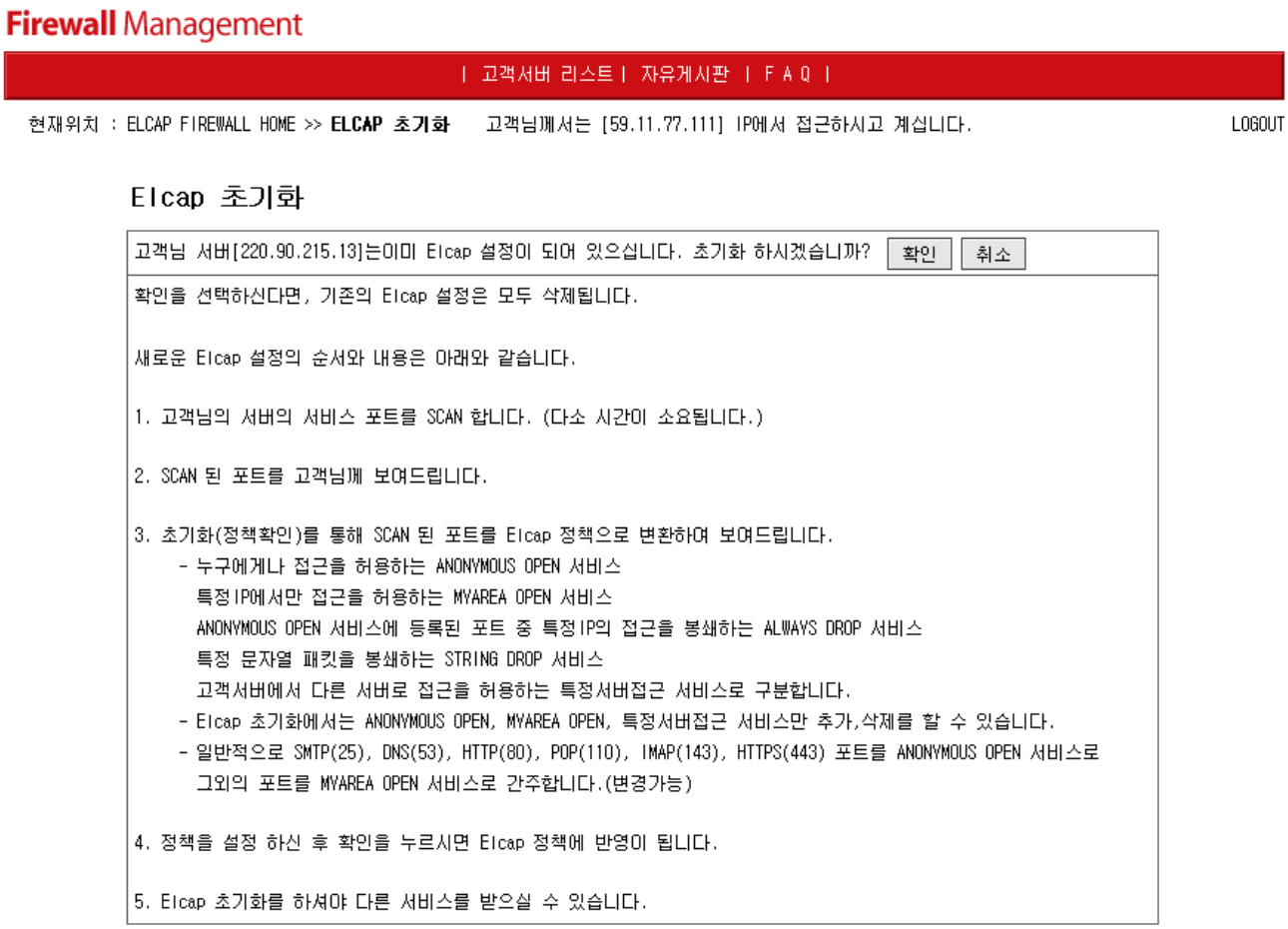
Elcap 해제 [#그림 2.1]



설명

- 기존에 등록된 정책을 모두 해제(삭제)하는 메뉴입니다.
- 기존에 등록된 정책을 해제시 서버는 모든 패킷을 허용합니다.

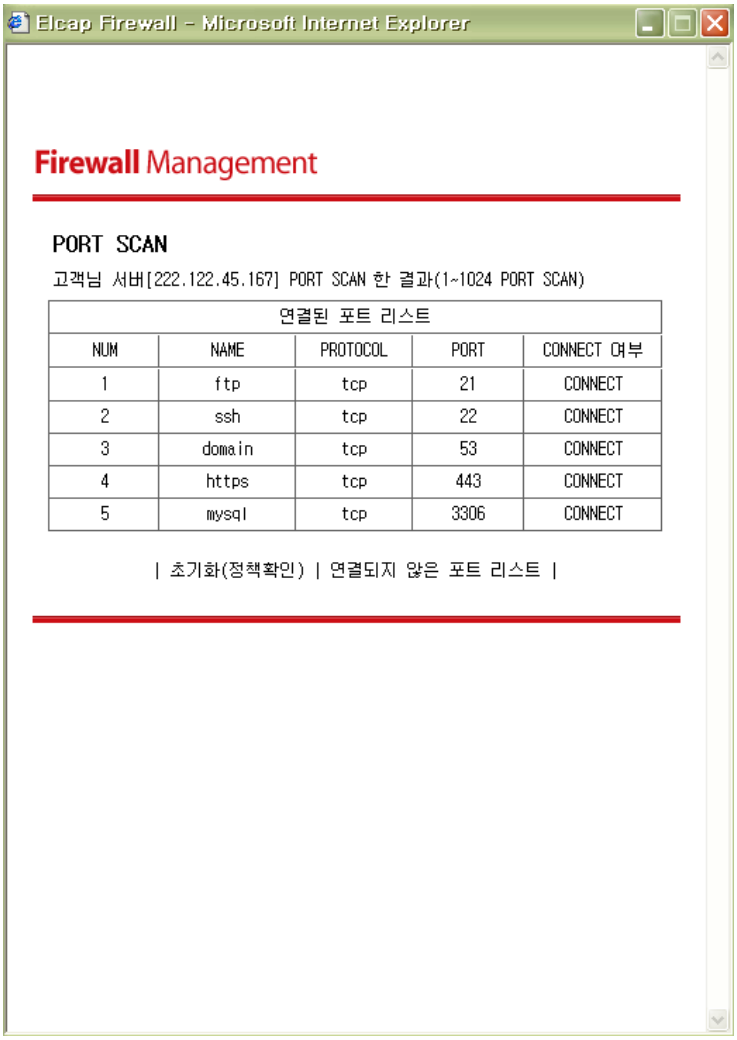
Elcap 초기화(Part1) [#그림 3.1]



설명

- 기본적으로 SMTP(25), DNS(53), HTTP(80),POP(110),IMAP(143) HTTPS(443) 을 ANONYMOUS OPEN 정책으로 반영되나 변경할 수 있습니다.
- 그 외의 포트들은 MYAREA OPEN 정책입니다.

Elcap 초기화 (Part2) [#그림 3.2]



설명

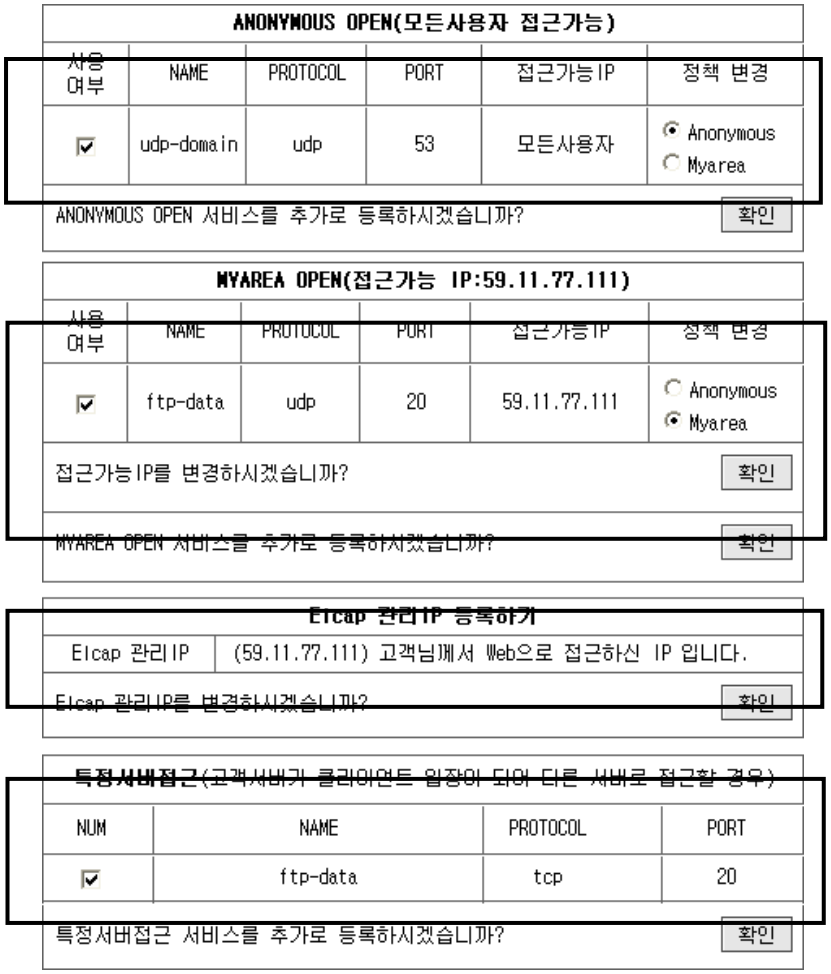
- 고객서버를 PortScan 한 후 Connect 된 포트를 보여줍니다.
- 초기화(정책확인)를 클릭하면, Connect 된 포트들을 Elcap Firewall 정책으로 변환시킵니다.
- 연결되지 않은 포트 리스트를 클릭하면, Connect 되지 않은 포트를 보여준다.

Elcap 초기화 (Part3) [#그림 3.3]

설명

- Connect 된 서비스(포트)를 ANONYMOUS OPEN, MYAREA OPEN, 특정서버접근 정책으로 변환시킨 화면입니다.
- Elcap Firewall 정책 추가, 변경, 삭제가 가능합니다.

Elcap 초기화 (Part3 - Detail) [#그림 3.3.1]



설명

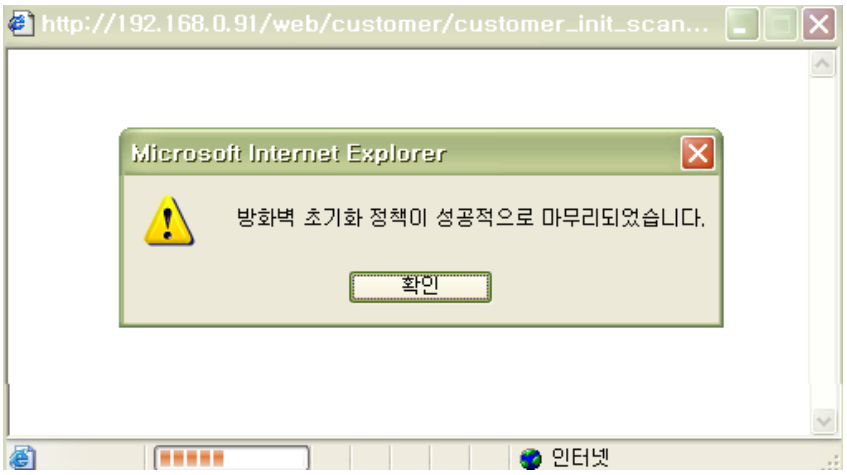
사용여부 - 해당 포트를 정책에 반영한다면 Check
(ANONYMOUS OPEN, MYAREA OPEN, 특정서버접근이 이에 해당합니다.)

정책변경 - ANONYMOUS OPEN <====> MYAREA OPEN 정책으로 서로 변경합니다.
(ANONYMOUS OPEN, MYAREA OPEN이 이에 해당합니다.)

확인 - ANONYMOUS OPEN : ANONYMOUS OPEN 정책을 등록할 때 사용
- MYAREA OPEN : MYAREA OPEN 정책을 등록할 때 사용
- 접근가능IP : MYAREA OPEN 정책의 접근가능IP를 변경할 때 사용
- Elcap 관리IP=>MANAGE IP : 등록된 MANAGE IP 정책을 등록할 때 사용
- 특정서버접근 : 특정서버접근 정책을 등록할 때 사용

참고) 접근가능IP, MANAGE IP 등록은 IP 입력뿐 아니라, IP 대역도 입력 가능합니다.
IP대역 입력은 APPEND A를 참고 하십시오.

Elcap 초기화(Part4) [#그림 3.4]



설명

- Elcap Firewall에 정책이 적용이 되고 그 결과값을 고객에게 보여줍니다.

Elcap 정책설정 (ANONYMOUS OPEN, ALWAYS DROP) [#그림 4.1]

Firewall Management

| 고객서버 리스트 | 자유게시판 | F A Q |

현재위치 : ELCAP FIREWALL HOME >> Elcap 정책설정 >> **ANONYMOUS OPEN | ALWAYS DROP** LOGOUT

고객님께서는 [59.11.77.113] IP에서 접근하시고 계십니다.

Elcap 정책설정

ANONYMOUS OPEN 정책

No	서비스 이름	포트	프로토콜	삭제
1	http	80	tcp	[삭제]
2	imap	143	tcp	[삭제]

이전◀ [1] ▶다음 추가하기

ALWAYS DROP 정책

No	서비스 이름	포트	프로토콜	DROP 접근 IP		삭제
1	http_drop	80	tcp	222.122.122.121 222.122.122.122	[개별삭제] [개별삭제]	[삭제]

이전◀ [1] ▶다음 추가하기

정책이동 => | ANONYMOUS OPEN | ALWAYS DROP | MYAREA OPEN | 특정서버접근 | MANAGE IP |

설명

- 정책설정은 5가지로 나뉘어 집니다.

1) ANONYMOUS OPEN : 접근IP가 어떤 것이든 상관없이 등록된 포트로 들어오는 패킷을 모두 허용합니다

1. No - ANONYMOUS OPEN에 설정된 Number를 의미합니다.
2. 서비스 이름 - 포트에 해당하는 이름을 의미합니다. 영문(1 ~ 30자), 한글(1~15자)
3. 포트 - 숫자로 된 포트를 의미합니다.(1 ~ 65535 범위의 포트 중 하나)
4. 프로토콜 - TCP, UDP, ICMP 서비스로 나뉩니다.
5. 정책변경/삭제 - [MYAREA OPEN]은 해당 포트를 MYAREA OPEN 정책으로 변경합니다.
   - 삭제는 해당 포트를 정책에서 삭제합니다. (해당 포트가 ALWAYS DROP 정책에 등록이 되어 있다면, 등록되어 있는 포트도 자동 삭제됩니다.

2) ALWAYS DROP : ANONYMOUS OPEN에 등록되어 있는 포트만 ALWAYS DROP에 등록할 수 있습니다.
(접근IP가 어떤 것이든 상관없이 접근을 허용하고 싶지만, 특정IP or 특정IP 대역에서는 접근을 봉쇄시켜야 할 경우 사용합니다.)
IP대역 입력은 APPEND A를 참고하십시오.

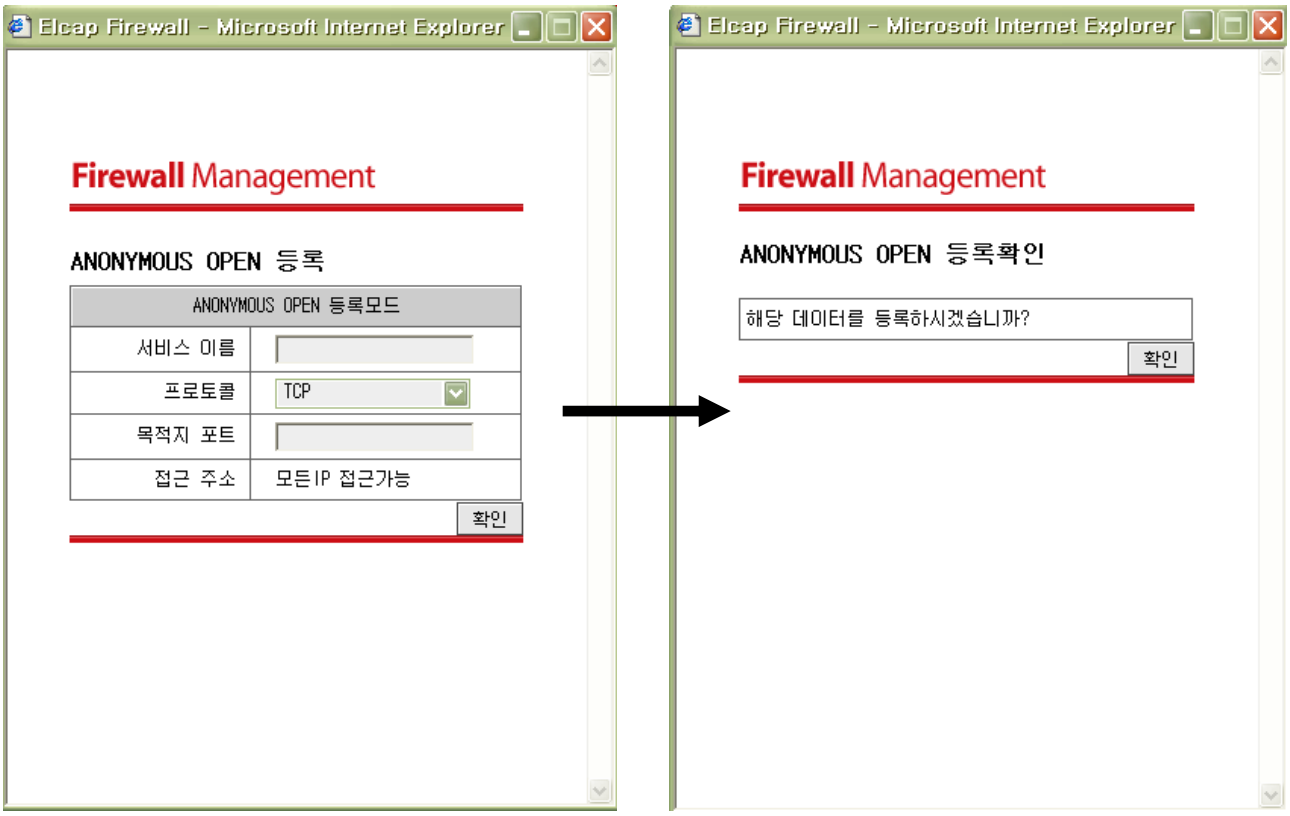
1. No - ALWAYS DROP에 설정된 Number를 의미합니다..
2. 서비스 이름 - 포트에 해당하는 이름을 의미합니다. 영문(1 ~ 30자), 한글(1~15자)
3. 포트 - 숫자로 된 포트를 의미합니다.(1 ~ 65535 범위의 포트 중 하나)
4. 프로토콜 - TCP, UDP, ICMP 서비스로 나뉩니다.
5. DROP 접근 IP - 해당 포트에 접근을 봉쇄할 IP 입니다. (IP or IP대역 입력가능)
   개별삭제 - 접근을 봉쇄할 IP or IP대역을 정책에서 개별로 삭제합니다.
6. 삭제 - 해당 포트를 정책에서 삭제합니다.

3) MYAREA OPEN

4) 특정서버접근

5) MANAGE IP

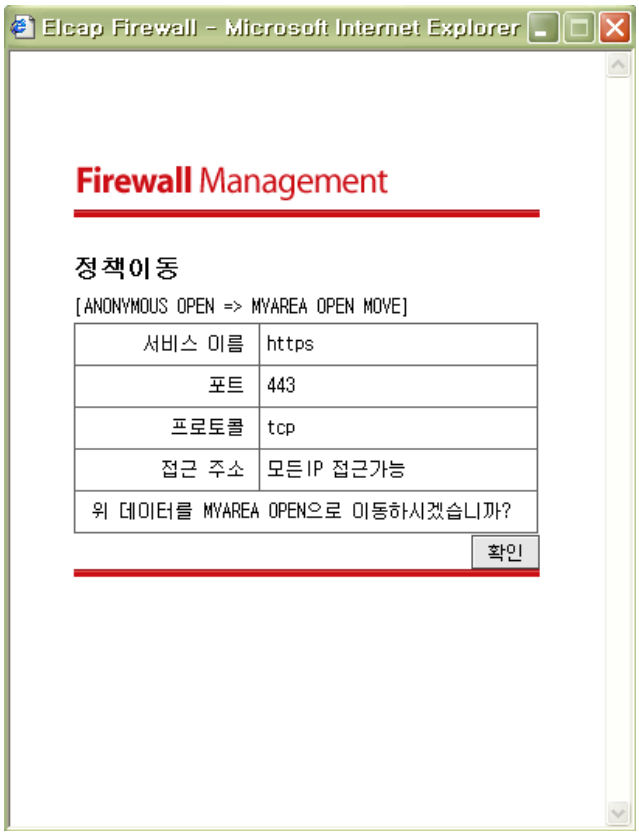
Elcap 정책설정 (ANONYMOUS OPEN 등록) [#그림 4.2]



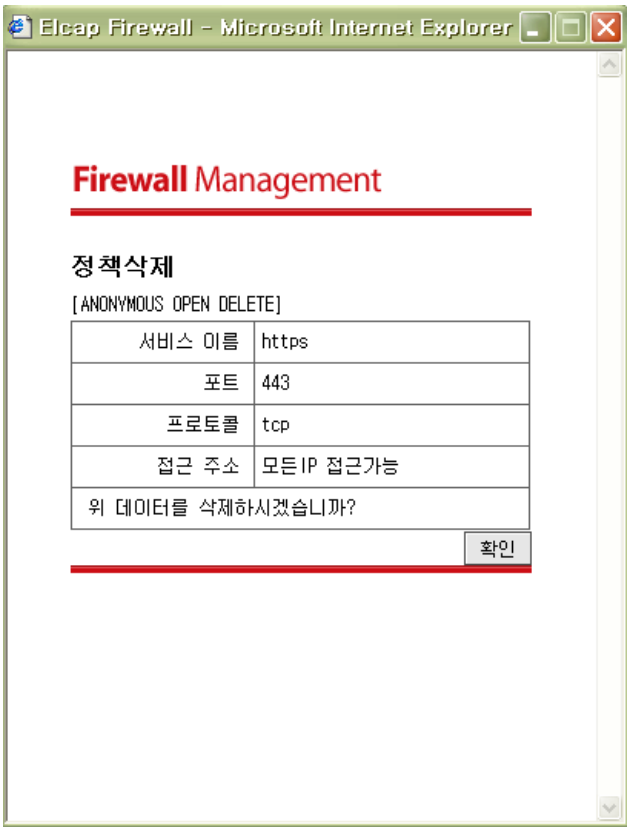
설명

1. 서비스 이름 – 고객이 입력할 서비스 이름(입력범위-한글:15자 이내, 영문30자 이내)
   ex) Ftp, Telnet, SSH
2. 프로토콜 - TCP, UDP, ICMP
   - TCP는 등록할 TCP 포트를 접근IP가 어떤 것이든 상관없이 모든이에게 허용시킵니다.
   - UDP는 등록할 UDP 포트를 접근IP가 어떤 것이든 상관없이 모든이에게 허용시킵니다.
   - ICMP는 ICMP를 접근IP가 어떤 것이든 상관없이 모든이에게 허용시킵니다.
   ex) 접근IP가 어떤 것이든 상관없이 외부에서 고객서버로 ping을 보낼수 있게 허용.
3. 목적지 포트 – 정책에 등록할 포트
4. 접근 주소 - 접근IP가 어떤 것이든 상관없이 모두가 접근 가능합니다.

Elcap 정책설정
(ANONYMOUS OPEN 정책이동) [#그림 4.3]



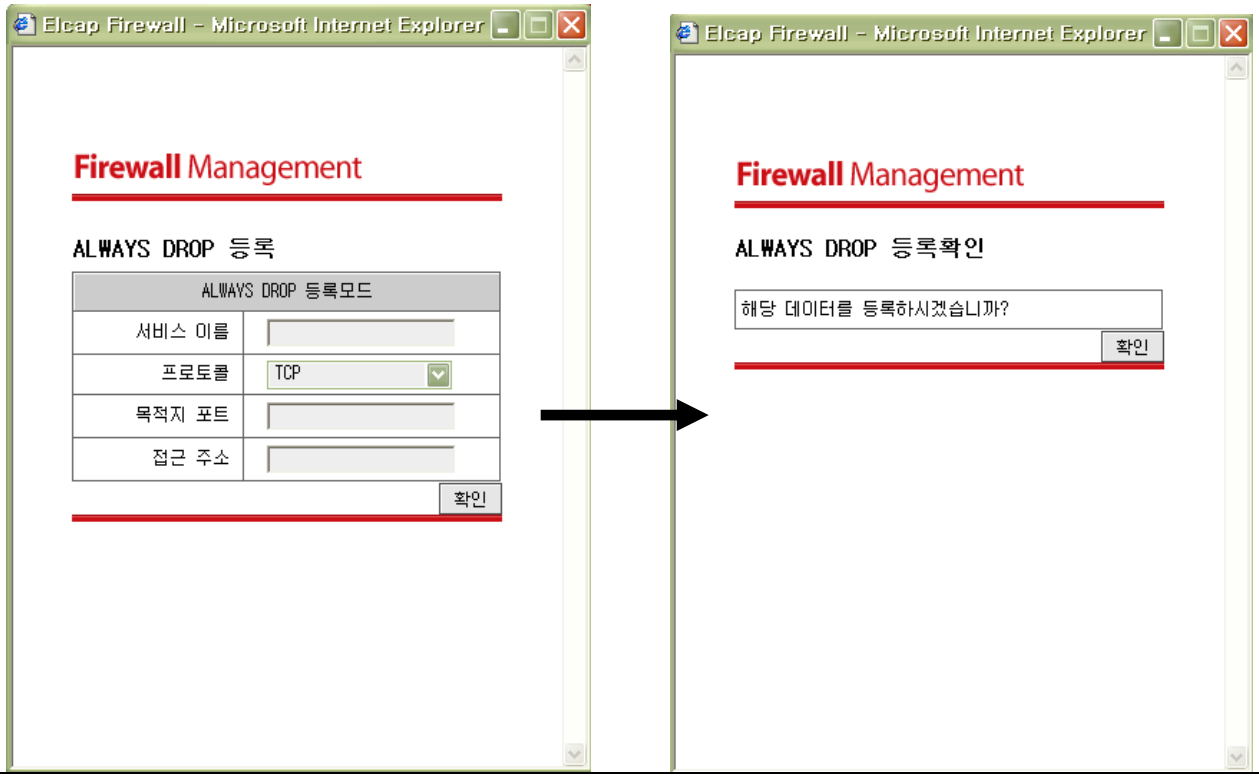
Elcap 정책설정
(ANONYMOUS OPEN 정책삭제) [#그림 4.4]



설명

- 정책이동 : ANONYMOUS OPEN => MYAREA OPEN으로 정책을 이동합니다.
  정책이동시 이동하는 포트가 ALWAYS DROP에 등록이 되어 있다면, 정책에서 삭제 됩니다.
- 정책삭제 : ANONYMOUS OPEN의 정책을 삭제합니다.
  정책삭제시 삭제하는 포트가 ALWAYS DROP에 등록이 되어 있다면, 정책에서 삭제 됩니다.

Elcap 정책설정 (ALWAYS DROP 등록) [#그림 4.2]

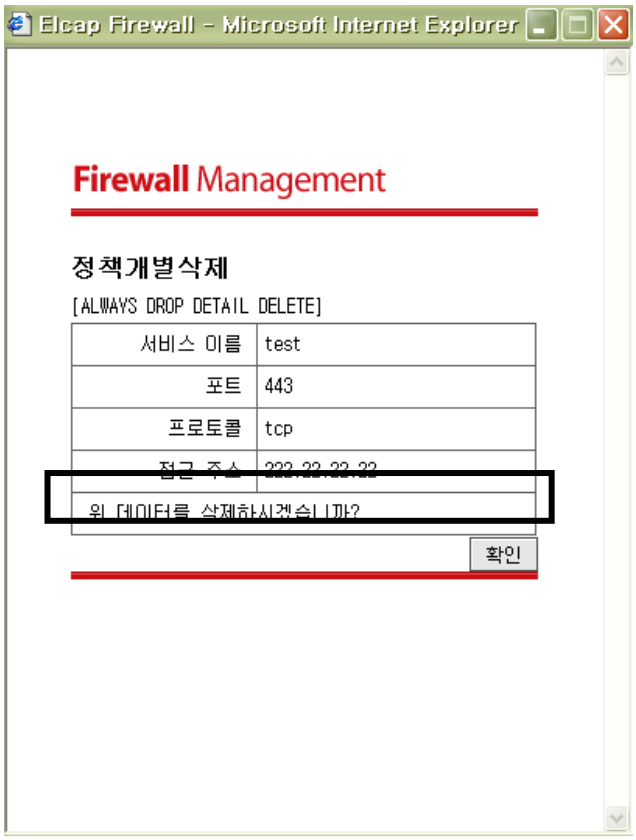


설명

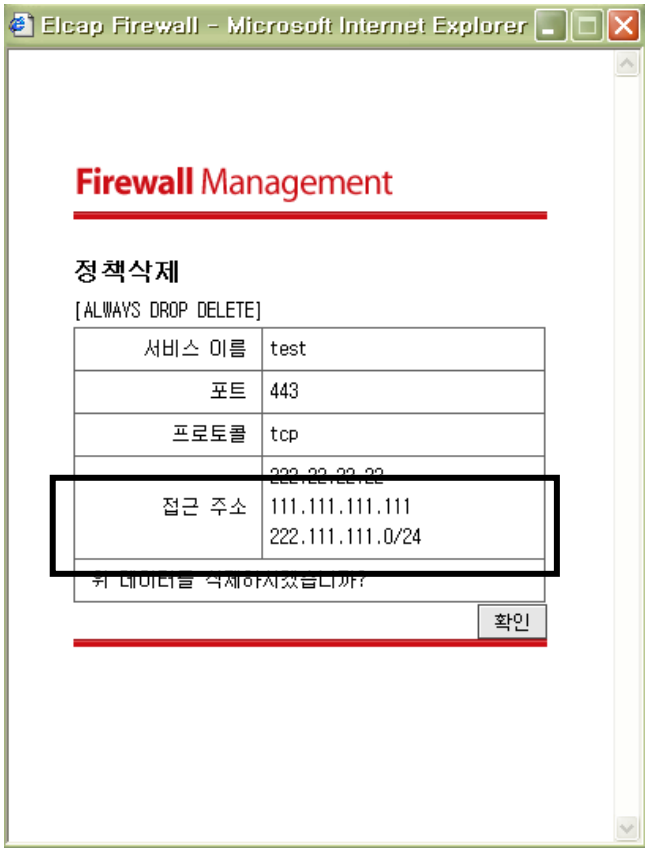
- ALWAYS DROP는 ANONYMOUS OPEN에 등록되어 있는 포트만 입력이 가능합니다.
- 접근IP가 어떤 것이든 상관없이 등록된 포트로 들어오는 패킷을 모두 허용하지만,
  특정접근IP 또는 IP대역에서 패킷을 봉쇄하여야 할 때 사용합니다.

1. 서비스 이름 – 고객이 입력할 서비스이름(입력범위-한글:15자 이내, 영문32자 이내)
   ex) Ftp, Telnet, Ssh
2. 프로토콜 - TCP, UDP, ICMP
   - TCP는 등록할 TCP 포트를 접근IP가 어떤 것이든 상관없이 모든이에게 허용하지만,
     등록할 IP or IP 대역에서는 봉쇄시킵니다.
   - UDP는 등록할 UDP 포트를 접근IP가 어떤 것이든 상관없이 모든이에게 허용하지만,
     등록할 IP or IP 대역에서는 봉쇄시킵니다.
   - ICMP는 ICMP 프로토콜을 접근IP가 어떤 것이든 상관없이 모든이에게 허용하지만,
     등록할 IP or IP 대역에서는 봉쇄시킵니다.
   ex) 외부에서 고객서버로 ping을 보낼수 있지만, 등록할 IP에서는 ping을 막습니다.
3. 목적지 포트 – 정책에 등록할 포트
4. 접근 주소 - 포트를 봉쇄시킬 IP 및 IP 대역을 입력 (IP대역 입력은 APPEND A를 참고 하십시오.)

Elcap 정책설정
(ALWAYS DROP 개별삭제) [#그림 4.5]



Elcap 정책설정
(ALWAYS DROP 삭제) [#그림 4.4]



설명

- 정책개별삭제 : 해당포트에 포함되어 있는 해당 IP or IP 대역을 정책에서 개별 삭제합니다.
- 정책삭제 : 해당포트에 포함되어 있는 모든 IP or IP 대역을 정책에서 모두 삭제합니다.

Elcap 정책설정(MYAREA OPEN) [#그림 4.1]

설명

1) ANONYMOUS OPEN

2) ALWAYS DROP

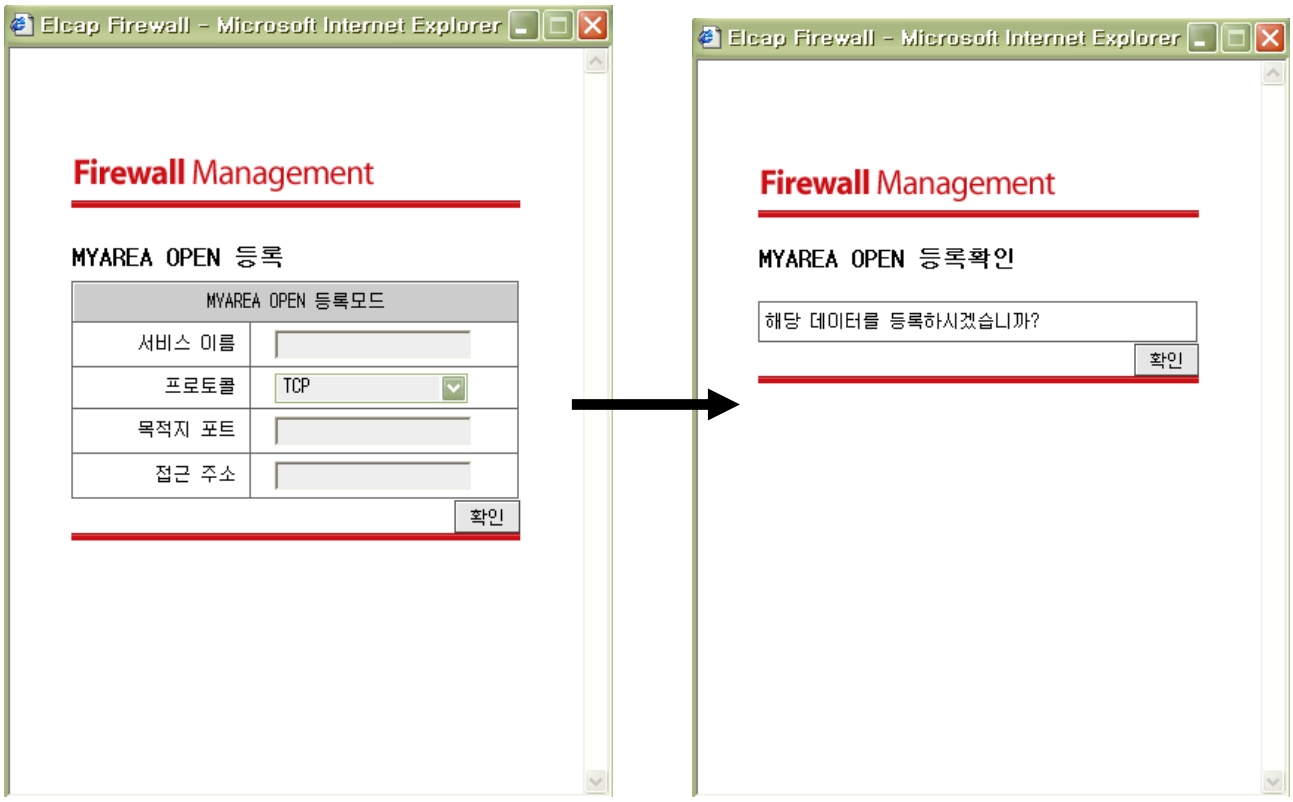
3) MYAREA OPEN - 특정IP or IP대역 에서만 서비스를 받을 수 있는 정책이다.

1. No - MYAREA OPEN에 설정된 Number를 의미합니다..
2. 서비스 이름 - 포트에 해당하는 이름을 의미합니다. 영문(1 ~ 30자), 한글(1~15자)
3. 포트 - 숫자로 된 포트를 의미합니다.(1 ~ 65535 범위의 포트 중 하나)
4. 프로토콜 - TCP, UDP, ICMP 서비스로 나뉩니다.
5. MYAREA접근IP - 해당 포트에 접근을 허용할 IP 입니다. (IP or IP 대역 입력가능)
   개별삭제 - 접근을 허용할 IP or IP대역을 정책에서 개별로 삭제합니다.
6. 삭제 - 해당 포트를 정책에서 삭제합니다.

4) 특정서버접근

5) MANAGE IP

Elcap 정책설정 (MYAREA OPEN 등록) [#그림 4.2]

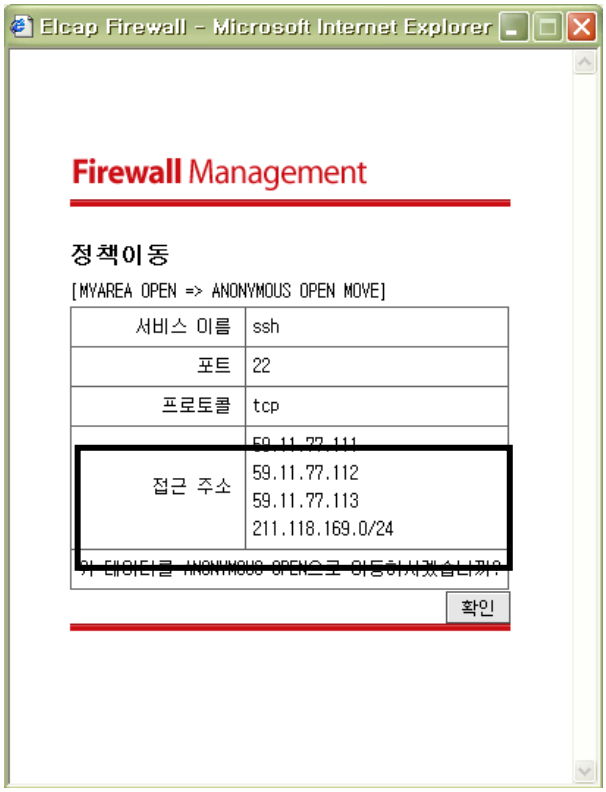


설명

- MYAREA OPEN는 ANONYMOUS OPEN에 등록되지 않은 포트만 등록가능합니다.

1. 서비스 이름 – 고객이 입력할 서비스 이름(입력범위-한글:15자 이내, 영문30자 이내)
   ex) Ftp, Telnet, Ssh
2. 프로토콜 - TCP, UDP, ICMP
   - TCP는 등록할 TCP 포트를 등록할 IP or IP대역에서 접근을 허용시킵니다.
   - UDP는 등록할 UDP 포트를 등록할 IP or IP대역에서 접근을 허용시킵니다.
   - ICMP는 ICMP 프로토콜을 등록할 IP or IP대역에서 접근을 허용시킵니다.
   ex) 등록할 IP or IP대역에서만, 고객서버로 ping을 보낼수 있게 허용합니다.
3. 목적지 포트 – 정책에 등록할 포트
4. 접근 주소 - 포트를 허용시킬 IP 및 IP대역을 입력 (IP대역 입력은 APPEND A를 참고 하십시오.)

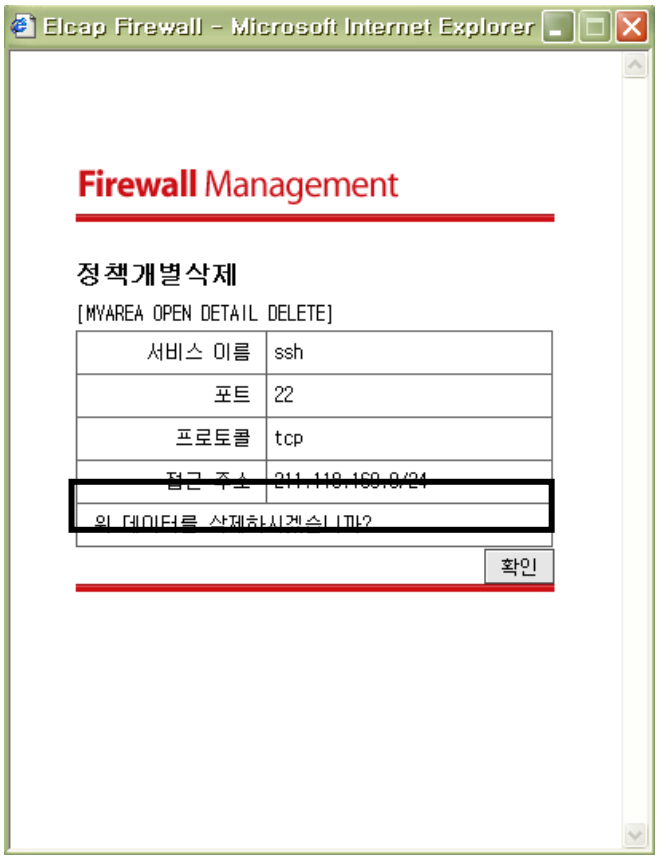
Elcap 정책설정 (MYAREA OPEN 정책이동) [#그림 4.3]



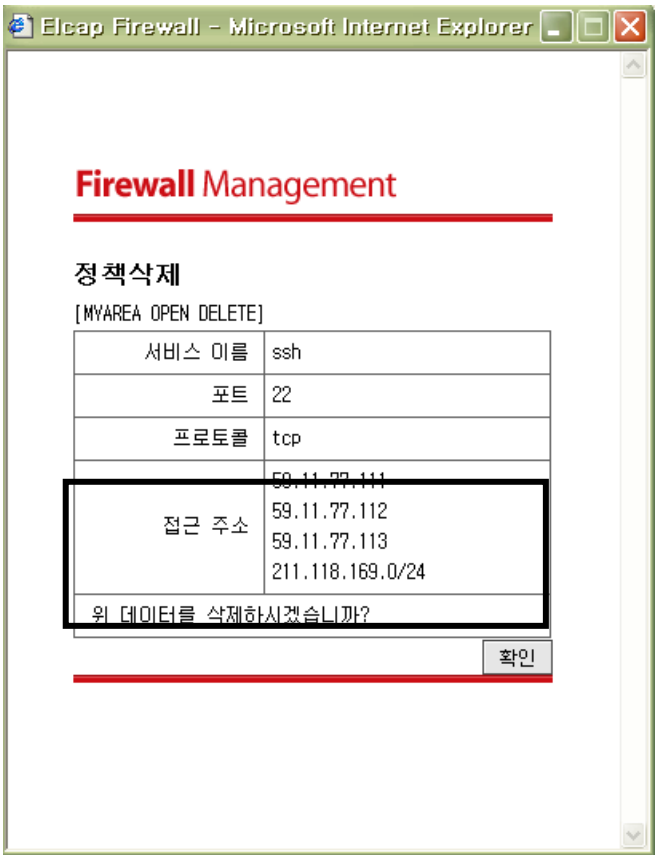
설명

- 정책이동 : MYAREA OPEN => ANONYMOUS OPEN 으로 정책을 이동합니다.

Elcap 정책설정
(MYAREA OPEN 개별삭제) [#그림 4.5]



Elcap 정책설정
(MYAREA OPEN 삭제) [#그림 4.4]



설명

- 정책개별삭제 : 해당포트에 포함되어 있는 해당 IP or IP 대역을 정책에서 개별 삭제합니다.
- 정책삭제 : 해당포트에 포함되어 있는 모든 IP or IP 대역을 정책에서 모두 삭제합니다.

Elcap 정책설정 (특정서버접근) [#그림 4.1]

설명

- 정책설정은 5가지로 나뉩니다.

1) ANONYMOUS OPEN , 2) ALWAYS DROP, 3) MYAREA OPEN

4) 특정서버접근

- 위 3가지 정책은 고객서버로 어떤이가 접근할 때의 정책이고, 특정서버접근은 고객서버에서 다른서버로 접근할 때의 정책입니다. (즉 위 3 가지 정책은 고객서버가 서버의 입장에서의 정책, 특정서버접근은 고객서버가 클라이언트 입장에서의 정책입니다.)

예를 들어

고객서버에서 다른 FTP서버로 접근할 경우 및 데이터를 받을 경우

고객서버에서 다른 HTTP서버로 접근할 경우 및 데이터를 받을 경우

고객서버에서 Microsoft 서버에 접속하여 Window Update 할 경우

고객서버에서 다른 서버로 접근하는 서비스(포트)를 등록시켜야 합니다.

일반적으로 Window는

FTP(TCP 20포트, TCP 21포트, UDP 20포트, UDP 21포트), SMTP(TCP 25포트),

DNS (TCP 53포트, UDP 53포트), HTTP(TCP 80포트),

Netbios-ssn(TCP 139포트) – Window directory service, Web-ssl(TCP 443포트),

Ms-sql(TCP 1433포트), MSN(TCP 1864포트), 인터넷품질테스트(TCP 8020포트, TCP 8031포트)

Unix, Linux는

FTP(TCP 20 포트 , TCP 21 포트, UDP 20 포트), SMTP(TCP 25 포트), TIME(TCP 37 포트),

WHOIS(TCP 43 포트), DNS (TCP 53 포트, UDP 53 포트),HTTP(TCP 80 포트), Web-ssl(TCP 443 포트),

를 등록시켜 주어야 고객서버에서 다른 서버로 접근이 가능합니다.

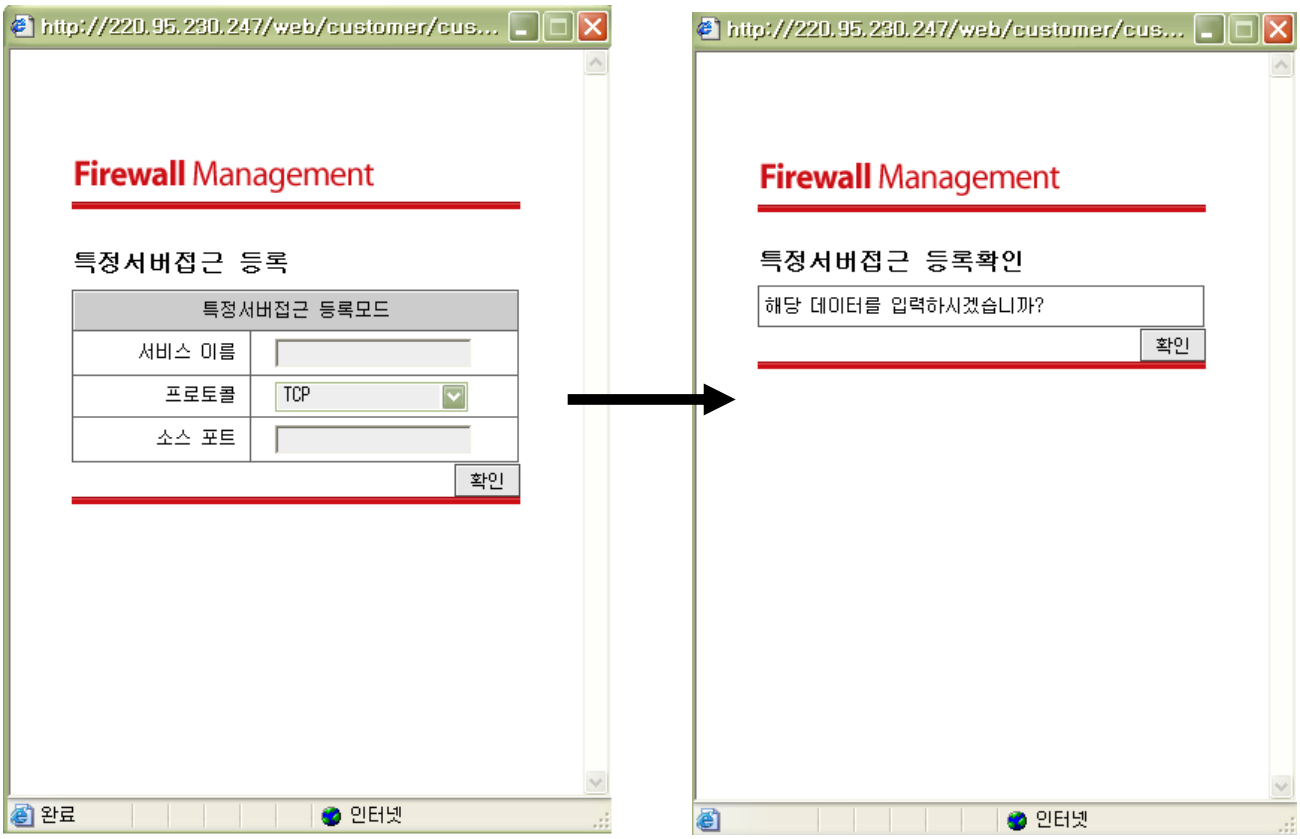
주) Elcap 초기화를 할 경우 위 포트들은 자동적으로 정책에 추가됩니다.

혹 고객서버에서 다른서버로 접근이 가능하지 않을 경우, 다른서버의 서비스 포트를

특정서버접근에 등록되었는지 다시 한번 확인하여 주십시오.

5) MANAGE IP

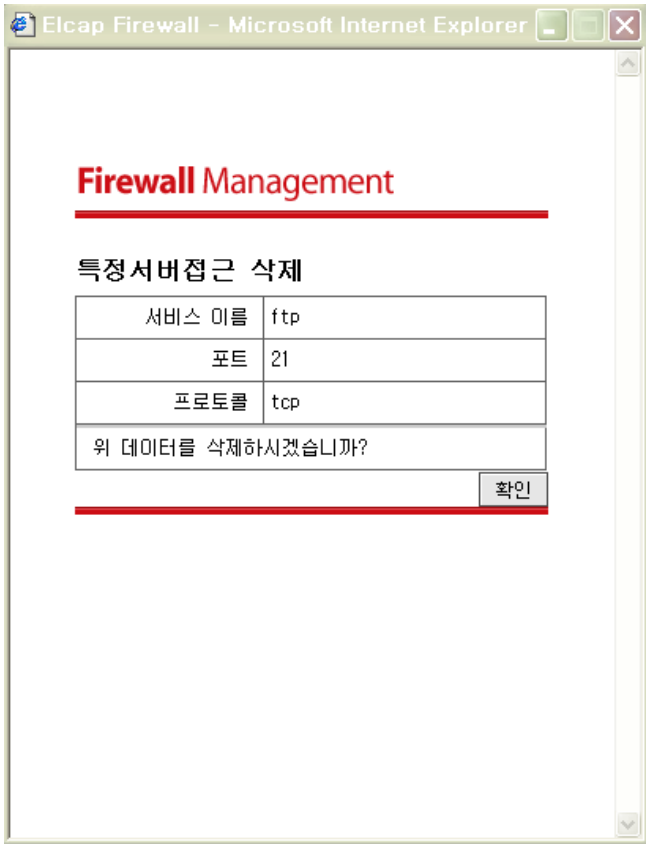
Elcap 정책설정 (특정서버접근 등록) [#그림 4.2]



설명

- 정책등록 : 특정서버접근 포트를 등록시킵니다.

Elcap 정책설정 (특정서버접근 삭제) [#그림 4.3]



설명

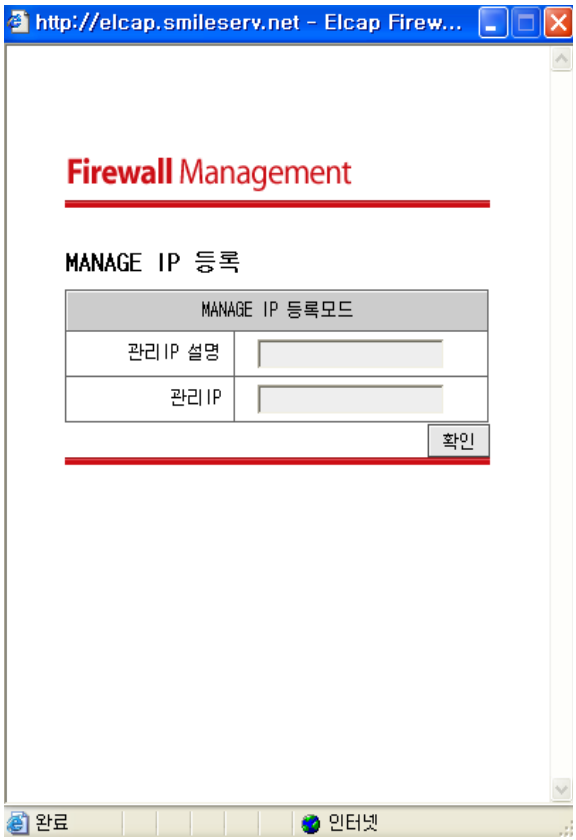
- 정책삭제 : 해당포트를 정책에서 삭제합니다.
  예를 들어 위의 그림처럼 21 포트를 삭제한다면, 고객서버에서 다른 서버 TCP 21 포트로 접근 할 수 없습니다. (기술적인 설명은 FAQ를 참조하여 주십시오.)

Elcap 정책설정(MANAGE IP) [#그림 4.1]

설명

1) ANONYMOUS OPEN
2) ALWAYS DROP
3) MYAREA OPEN
4) 특정서버접근
5) MANAGE IP
   - 위 4가지 정책은 포트 기반의 정책이고, MANAGE IP 정책은 IP 기반의 정책입니다.
     등록된 IP는 서비스하는 모든 포트에 접근이 가능하게 됩니다.

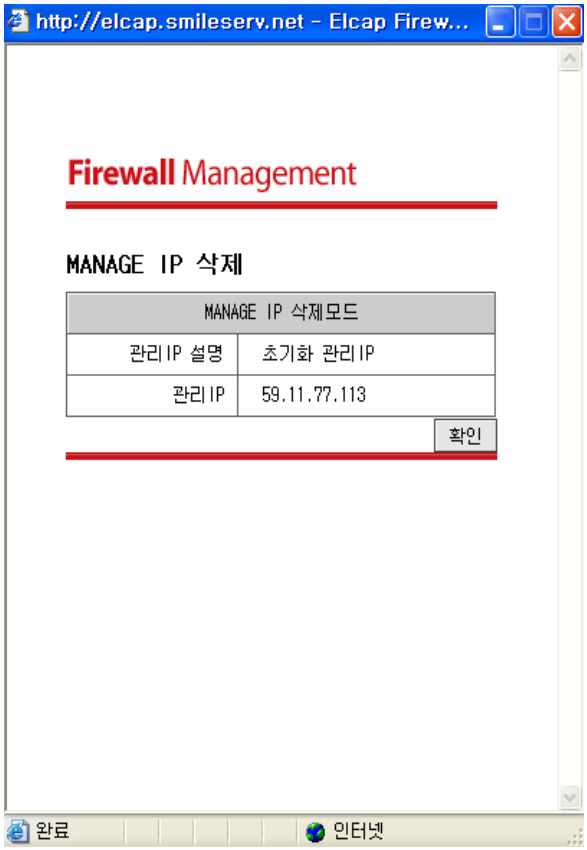
MANAGE IP등록 [#그림 4.2]



설명

1. 모든 포트에 접근 가능하게 할 IP를 등록

MANAGE IP삭제 [#그림 4.3]



설명

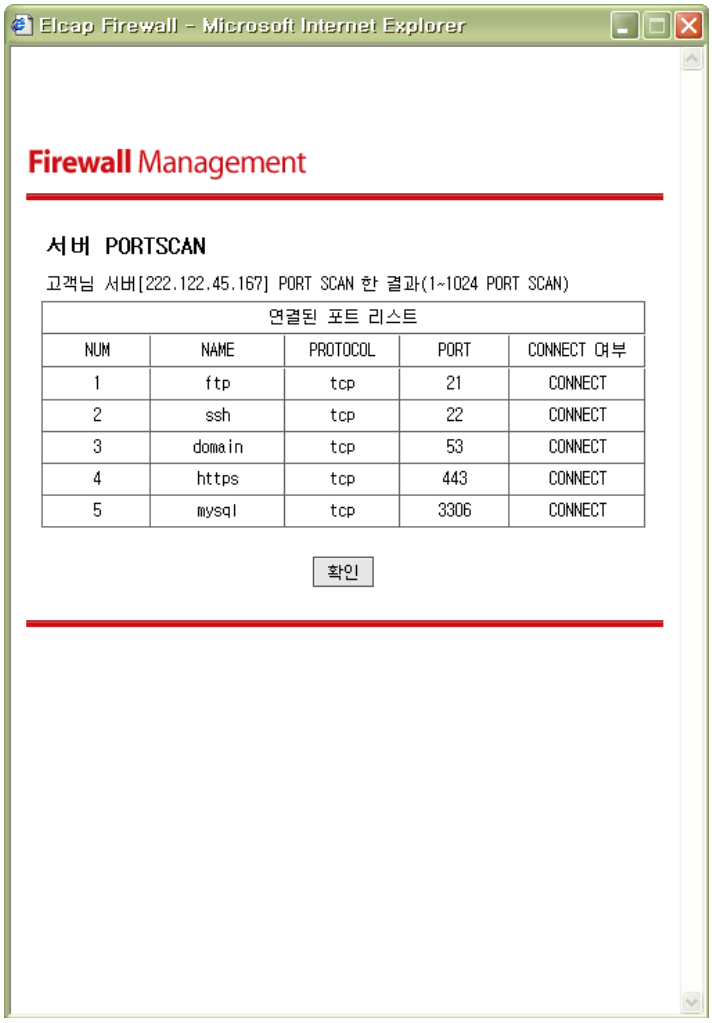
1. MANAGE IP를 삭제합니다.

Elcap 정책보기 [#그림 6]

설명

- 고객이 등록한 정책 보여주는 페이지입니다.

서버 PORTSCAN [#그림 7]



설명

- 정책이 설정된 상태에서 다시 PORTSCAN 하는 페이지입니다.

서버 PORTLIST [#그림 8]

설명

- 고객서버에 PORTSCAN 할 리스트를 보여줍니다.
- 운영체제별로 PORTSCAN 할 리스트가 다릅니다.

O S [#그림 9]

설명

- (주) Smileserv에서 서비스하고 있는 고객서버의 운영체제
- Unix Linux 계열, Window 계열, 스위치 계열 3가지가 있습니다.
- 스위치계열은 코로케이션 사용자만 해당합니다.
- OS를 변경하는 즉시 모든 정책을 모두 해제(삭제) 합니다.(즉 해당 서버는 모든 패킷을 허용합니다.)

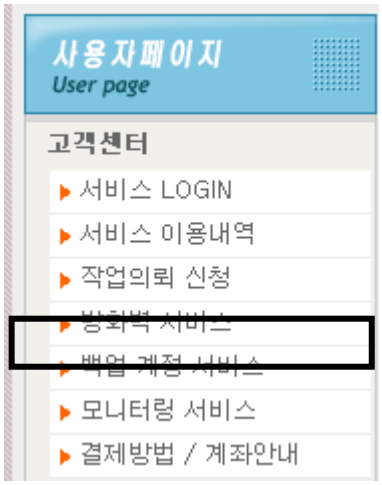
자유게시판

- Elcap Firewall에 대한 궁금증 or 문제점 등의 글을 올려주시면 저희가 궁금증은 답변을 통해 해결해 드리고 문제점은 고객님의 의견을 수렴하여 수정하도록 하겠습니다.

F A Q

- Elcap Firewall 있는 FAQ 내용과 동일합니다.
- 고객님들이 공통적으로 호소하시는 문제점만을 중점적으로 설명하는 메뉴입니다.

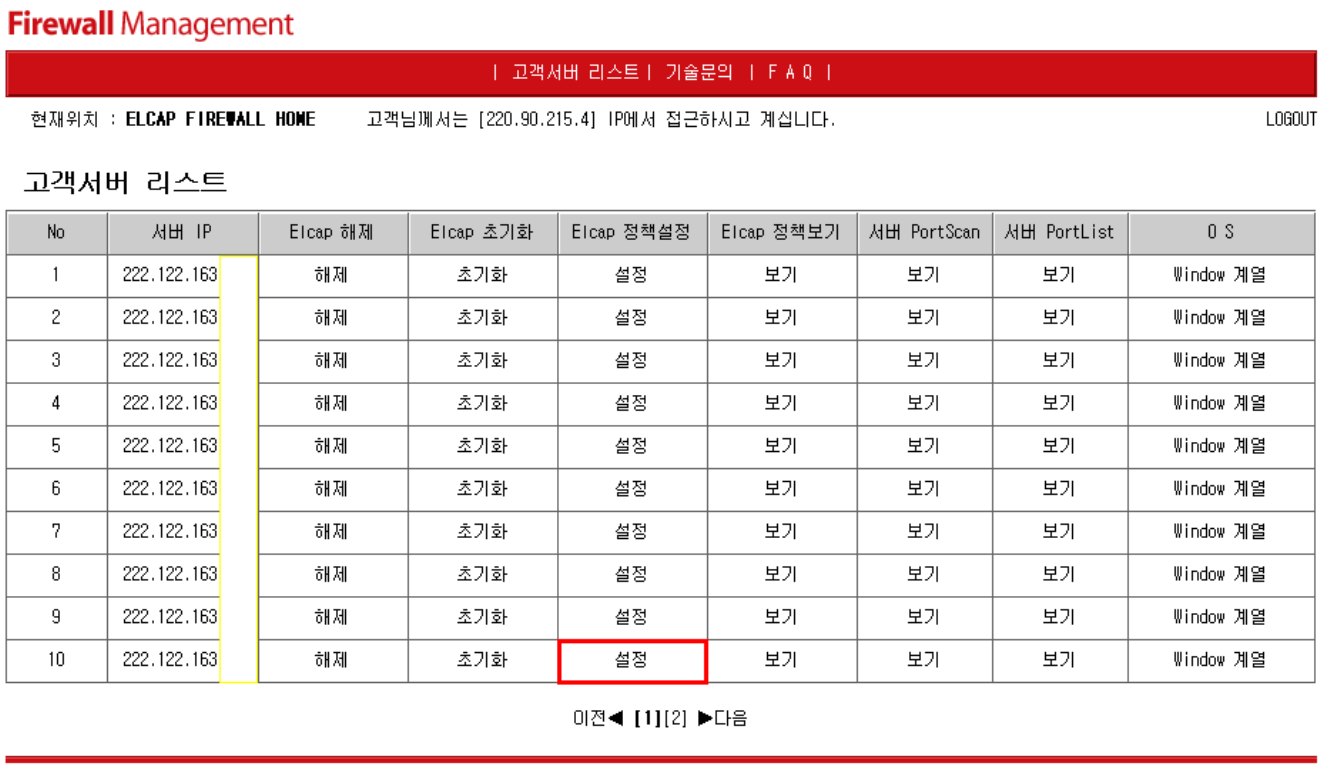
자동 Login



설명

- http://elcap.100dedi.com에 접속하시어 Login을 통하여 Elcap 정책을 추가하실 수 있습니다.
- http://www.100dedi.com에 Login 하신 후 “방화벽 서비스” 클릭하시면 별도의 인증 절차 없이 Login 이 가능합니다.

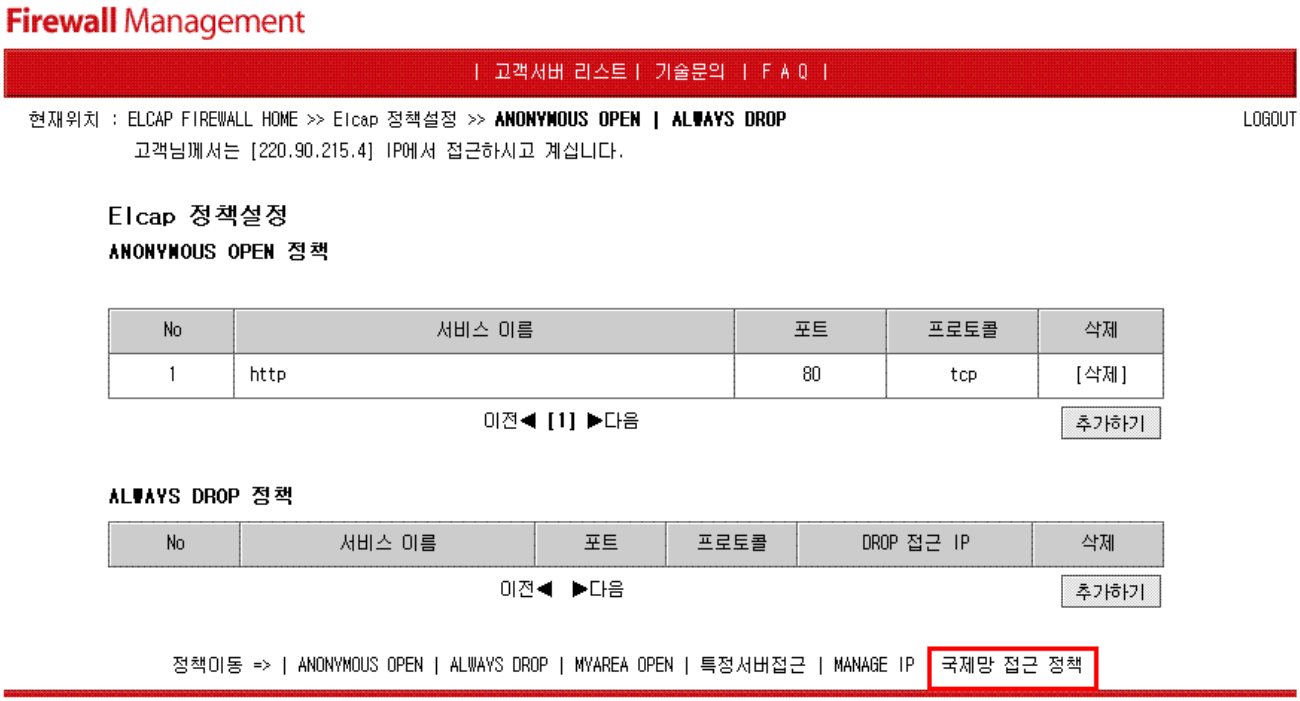
Elcap Firewall 국제망 정책 설정[#그림 5.1]



설명

1. Elcap 로그인 후 고객서버 리스트에서 [Elcap 방화벽 정책설정]을 클릭합니다.

Elcap Firewall 국제망 정책 설정[#그림 5.2]



설명

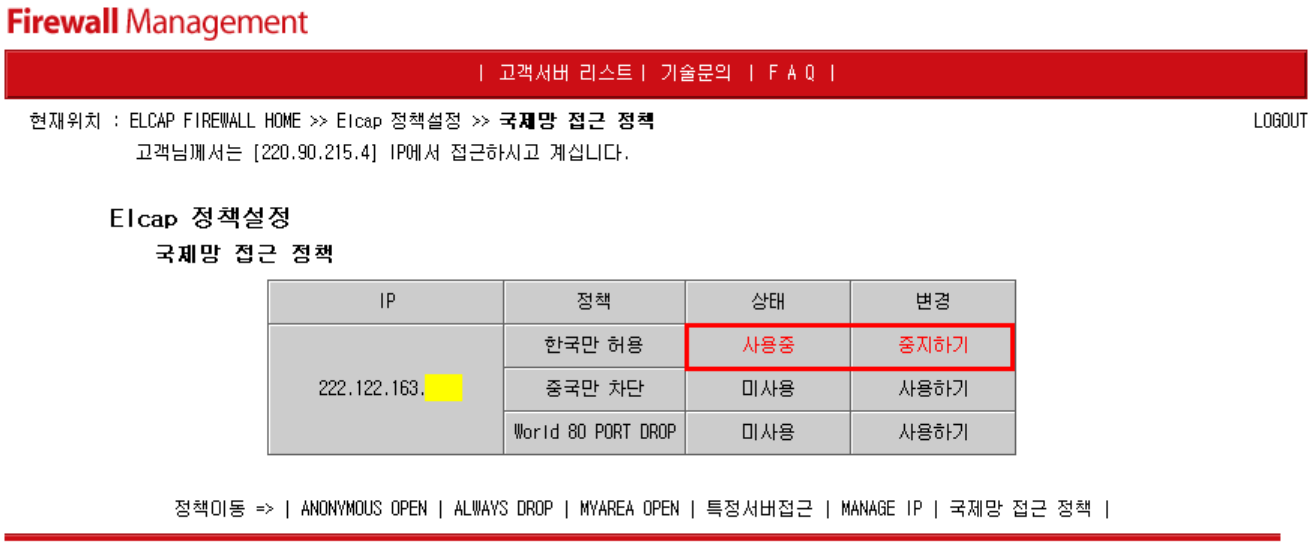
2. Elcap 방화벽 정책설정에서 [국제망 접근 정책]을 클릭합니다.

Elcap Firewall 국제망 정책 설정[#그림 5.3]

설명

3. 국제망 접근 정책에서 해당 정책에서 [사용하기]를 클릭합니다.
   아래의 3개 정책들은 각각 적용이 되므로 중복 적용이 가능합니다.

Elcap Firewall 국제망 정책 설정[#그림 5.4]



설명

4. 적용중인 정책은 아래와 같이 적색으로 상태가 바뀌어 표시되며,
   중지하기를 클릭하시면 해당 정책을 다시 중지 하실 수가 있습니다.

8. F A Q

Q-1) 서버에 접근을 할 수 없습니다.

A-1) 아래의 세가지 경우 중 하나에 포함이 될 것입니다.
첫번째는 고객님께서 서버에 접근하려는 IP(MYAREA OPEN, MANAGE IP)를 입력하신 후
서버에 접근하려는 IP가 변경된 경우(유동IP)

두번째는 고객님께서 Elcap Firewall을 설정을 하지 않으셨다면, 고객님 서버의
Elcap Firewall 정책은 입력되는 패킷 허용(ACCEPT), 출력되는 패킷 허용(ACCEPT)
즉 고객님 서버의 운영되는 서비스(포트)는 모두 허용되고 있습니다.
고객님서버의 문제일 가능성이 높습니다.

세번째는 고객님께서 Elcap Firewall을 설정하셨다면, 고객님이 고객님서버에 접근하는 IP를
잘못입력하셨거나, 고객님 서버의 문제일 가능성이 높습니다.

두번째와 세번째의 경우는
스마일서브(031-701-5134~5)에 전화를 주셔서 서버의 상태확인을 요청하십시요.

Q-2) 서버에 접속이 되며, 또한 서버의 서비스도 정상적으로 운영되고 있습니다.
그런데, 제 서버에서 다른 서버로 접속이 되지 않습니다. 왜 그런 건가요?

A-2) Elcap Firewall 정책은 크게 5가지로 되어 있습니다.
ANONYMOUS OPEN, MYAREA OPEN, ALWAYS DROP, 특정서버접근, MANAGE IP
위 3가지는 고객서버의 서버 정책을 세우는 것이고(고객서버로 어떤이가 접근할 때의 정책),

특정서버접근는 고객서버가 클라이언트로써의 정책을 세우는 것입니다.
(고객서버에서 다른서버로 접근할 때의 정책).

예를 들면
고객님 서버에서 Window Update를 할 경우(고객님 서버 운영체제가 Window일 때)
- 고객님 서버에서 MicroSoft Server의 tcp 80번 포트와 데이터를 받는
udp or tcp 20번 포트로 통신.
- 특정서버접근에 tcp 80번과 tcp 20번과 udp 20번을 등록합니다.

고객님 서버에서 다른 서버로 FTP를 통해 데이터를 업로드 또는 다운로드 받을 경우
- 고객님 서버에서 다른 서버의 tcp 21번 포트와 udp or tcp 20번 포트로 통신을
해야 합니다.
- 특정서버접근에 tcp 21번과 tcp 20번과 udp 20번을 등록합니다.

이럴 경우에 [특정서버접근]에 접근하려는 포트를 입력시켜 주어야 통신을 할 수 있습니다.
그렇지만, 일반적으로 [Elcap 초기화]를 할 경우 운영체제별로 필요한 특정서버접근 포트를 자동적으로 입력 시켜줍니다.
고객서버에서 외부로 접근을 할 수 없다면, 외부의 서버가 서비스되고 있지 않던가 아님 고객님께서 [특정서버접근] 에서 해당 포트를 정책에서 삭제하셔서 외부로 접근하지 못하는 것입니다.
이런 경우에는 Elcap 정책설정 메뉴의 설정(클릭)=>특정서버접근(클릭)=>해당포트를 입력하여 주시면, 외부에 접근이 가능해집니다.

일반적으로 Window는
FTP(TCP 20포트 , TCP 21포트, UDP 20포트), SMTP(TCP 25포트),
DNS(TCP 53포트, UDP 53포트), HTTP(TCP 80포트),
인터넷품질테스트(TCP 8020,8031포트), Netbios-ssn(TCP 139포트),
Web-ssl(TCP 443포트), Ms-sql(TCP 1433포트), MSN(TCP 1864포트)

Unix, Linux는
FTP(TCP 20포트 , TCP 21포트, UDP 20포트), TIME(TCP 37포트), SMTP(TCP 25포트),
WHOIS(TCP 43포트), DNS(TCP 53포트, UDP 53포트) HTTP(TCP 80포트),
Web-ssl(TCP 443포트)

Q-3) Elcap Firewall 정책설정이 어렵습니다. 정책설정을 도와주시면 안될까요?

A-3) Elcap Firewall 제작과정에서 가장 중요시 했던 사항은 고객님께서 알기 쉽도록 만드는 것이었습니다.
우선 고객님께서 메뉴얼을 한번 읽어 보시는 것이 좋을 듯 합니다.
메뉴얼을 한번 읽으신 후 정책을 세워보세요.

그래도 Elcap Firewall 정책설정이 어려우시다면, 아래의 설명대로 따라해 보세요.
1. 고객서버 리스트에서 Elcap 초기화를 클릭하여 주십시요.
2. Elcap 초기화 페이지에서 확인을 누르십시요.
3. 포트스캔이 되셨지요? 초기화(정책확인)를 누르십시요.
4. 정책확인 페이지에서 확인을 누르십시요.
5. 확인을 누르시면, 성공되었다고 나올것입니다.
6. 기본적인 Elcap Firewall 정책 설정은 되었습니다.
7. 고객님께서 서비스할 포트가 생겼다면, 정책 설정에서 추가시켜 주시면 됩니다.
8. 지금까지 설명드린 정책설정은 가장 기본적인 Elcap Firewall 정책설정이고, 메뉴얼을 보시면서 차근히 정책을 다듬어 보세요.

Elcap Firewall 정책 설정이 아직도 어려우시다면, 스마일서브로 연락을 주십시요.
Elcap Firewall 담당하시는 분께서 자세히 설명해 드릴 것입니다.

Q-4) 로그인 후 다른 페이지로 이동하면, 세션이 존재하지 않는다는 메시지가 나옵니다.
어떻게 해야 하죠?

A-4) 브라우져에 [인터넷 옵션]으로 들어가신 후 [개인 정보]로 들어 가시면, 개인 정보 설정이
보통으로 되어 있는지 확인을 하십시요.
보통으로 되어 있지 않다면, 보통으로 변경하시고, 확인을 누르십시요.
Logout 하신 후 브라우져를 모두 닫은 후 다시 Elcap Firewall에 로긴 하시면, 정상적으로
동작이 될 것입니다.
만약 그래도 되지 않는다면, 고객님 PC를 재부팅하시고 다시 접속해 보십시요.
간혹 CGI에서는 사용중인 메모리가 많으면, 세션이 잘 적용되지 않는 경우가 발생합니다.

Q-5) 제 서버의 운영체제가 틀려요. 어떻게 변경해야 하죠?
A-5) O S 메뉴를 선택하신 후 운영체제를 변경하시면 됩니다.
주의하실 점은 운영체제 변경을 하시면 그전에 모든 정책은 삭제됩니다.

Q-6) 메뉴얼의 내용이 너무 많아요. 정책에 관련된 사항을 간단하게 설명해 주세요.

A-6) 정책에 관련된 메뉴설명과 조작방법에 대해서 간단하게 설명드리겠습니다.

1. 고객님께서 아직 Elcap Firewall에 설정을 안 하셨다면,
고객서버의 정책은 All ACCEPT 입니다. 즉 모든 패킷을 허용합니다.
2. Elcap 해제
- 1번에서 설명드린 All ACCEPT 입니다.(즉 모든 패킷을 허용합니다.)
- [Elcap 해제]의 설정변경을 누르시고 Elcap 해제 페이지가 새창으로 뜨면
확인을 누르면 됩니다.
3. Elcap 초기화
- [Elcap 초기화] 의 초기화를 누르시면, Elcap 초기화 페이지가 뜨고,
아래에 설명이 나옵니다.
확인을 누르시면, 고객님 서버를 PortScan 하는 페이지가 나옵니다.
초기화(정책확인) 을 누르시면, PortScan 된 포트를 Elcap Firewall 정책으로
변경시키는 페이지가 나옵니다.
확인을 누르시면, Elcap Firewall 정책에 적용이 됩니다.
- ANONYMOUS OPEN 정책은 SMTP(25), DNS(53), HTTP(80), POP(110), IMAP(143), HTTPS(443)
이 포트이 해당되며, 나머지 포트는 MYAREA OPEN 정책에 해당됩니다.(변경가능)
특정서버접근은 고객님서버에서 외부서버로 접근할 경우 필요한 정책입니다.(변경가능)
- [Elcap 초기화] 단계를 거친 후에 다른 메뉴를 이용하실 수 있습니다.

4. Elcap 정책설정
- ANONYMOUS OPEN
누구나가 접근할 수 있는 서비스(포트)를 의미합니다.
ex) SMTP(25), DNS(53), HTTP(80), POP(110), IMAP(143), HTTPS(443)
- MYAREA OPEN

특정 IP에서만 접근할 수 있는 서비스(포트)를 의미합니다.
ex) FTP(20, 21), SSH(22), TELNET(23)

- ALWAYS DROP
ANONYMOUS OPEN에 등록되어 있는 서비스(포트)를 특정IP에서 접근할 수 없게 하는 정책입니다.
ex) 특정IP(210.154.145.13)에서 HTTP(80) 에 Attack을 가한다거나, 바이러스 패킷을 보낸다면, 모든 IP에서는 패킷을 ACCEPT 하나, 특정IP(210.154.145.13)를 DROP 시킬 수 있습니다.

- 특정서버접근
위 3가지 정책은 고객님 서버가 서버입장에서의 정책이고,
특정서버접근은 고객님 서버가 클라이언트 입장이 되었을 때의 정책이다.
예를 들어 고객님 서버에서 다른 외부 FTP서버를 이용할 경우
고객님 서버에서 다른 외부 HTTP서버를 이용할 경우
고객님 서버에서 Microsoft 서버에 접속하여 Window Update 할 경우
고객님 서버에서 다른 서버로 접근하는 서비스(포트)를 등록시켜야 합니다.

일반적으로 Window는
FTP(TCP 20포트 , TCP 21포트, UDP 20포트), SMTP(TCP 25포트),
DNS (TCP 53포트, UDP 53포트), HTTP(TCP 80포트),
인터넷품질테스트(TCP 8020,8031 포트)
Netbios-ssn(TCP 139포트) - Window directory service,
Web-ssl(TCP 443포트), Ms-sql(TCP 1433포트), MSN(TCP 1864포트)

Unix, Linux는
FTP(TCP 20포트 , TCP 21포트, UDP 20포트), TIME(TCP 37포트),
SMTP(TCP 25포트), WHOIS(TCP 43포트), DNS (TCP 53포트, UDP 53포트),
HTTP(TCP 80포트), Web-ssl(TCP 443포트)를 등록시켜 주어야 고객서버에서 다른서버로 접근을 할 수 있습니다.

특정서버접근 정책은 Elcap 초기화 단계에서 위 서비스(포트)를 자동적으로 등록시켜 줍니다.

- MANAGE IP
위 4가지 정책은 포트 기반의 정책이고, MANAGE IP는 IP 기반의 정책입니다.
MANAGE IP에 등록된 IP는 서비스 중인 모든 포트에 접근을 가능하게 해 줍니다.

5. Elcap 정책보기
- 고객님이 입력한 정책을 보여주는 메뉴입니다.

6. 서버 PortScan
- 고객님 서버를 PortScan 하는 메뉴입니다.

7. 서버 PortList
- 고객님 서버를 PortScan 할 Port 리스트 메뉴입니다.

8. OS
- 고객님 서버의 운영체제를 알려주는 메뉴입니다.(변경가능)

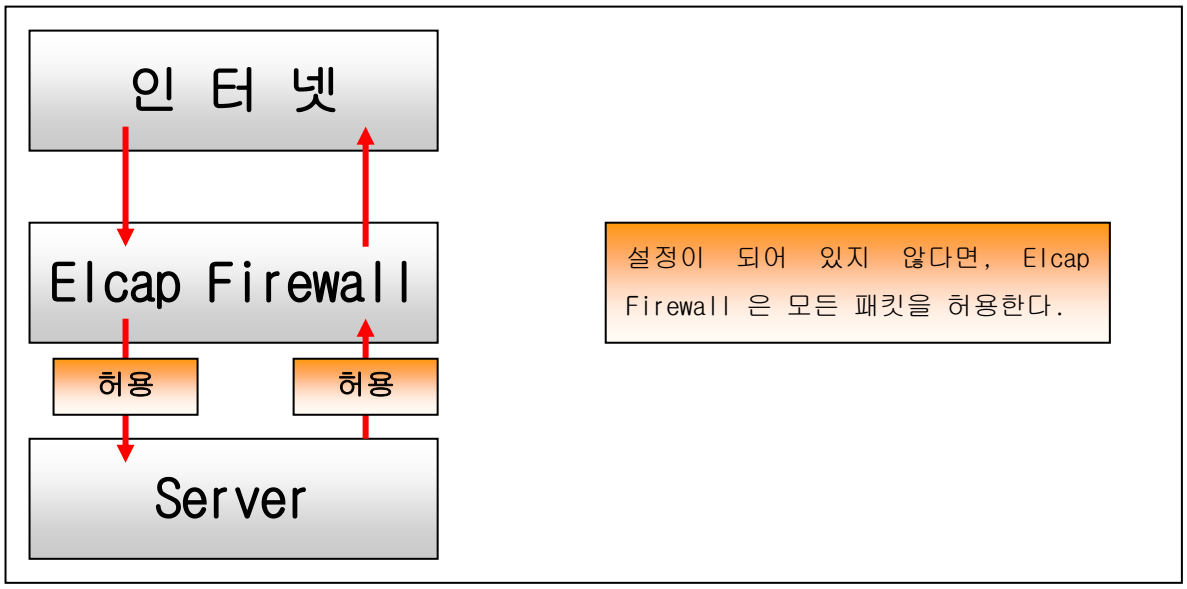
Q-7) 스마일서브에서 서버를 운영하고 있습니다.
신규고객만 Elcap Firewall 서비스를 받는 건가요? 아님
기존고객도 Elcap Firewall 서비스를 받나요?.
혹시 둘다 받을 수 있다면 Elcap Firewall을 어떻게 사용하나요?

A-7) 신규고객님 뿐만 아니라, 기존고객님들도 서비스를 받습니다.
두 고객님들은 현재 Elcap Firewall을 받고 계신 중입니다.
단, Elcap Firewall에 고객님 서버의 정책이 없을 뿐입니다.(Elcap Firewall 정책은 고객님들이 직접 세우셔야 합니다.)

Elcap Firewall 매뉴얼을 참고하여 정책을 세우시면 됩니다.
Elcap Firewall 개발에서 가장 중점을 둔 것은 고객님들이 이해하기 쉽게 만들었다는 점입니다. 일반적인 서버관리에 대한 개념을 가진 분이시면 쉽게 정책을 세우실 겁니다. 또한 처음 접하신 분이시라도 매뉴얼을 정독하시면 쉽게 정책을 세우실 겁니다.

Elcap Firewall 주소는 http://elcap.100dedi.com 입니다. (**#그림 1 참조**)
http://www.100dedi.com 에서 부여 받은 계정(id, password)으로 Login을 합니다.
Login 후 Elcap Firewall을 사용하시면 됩니다.

혹 Elcap Firewall에 설정을 아무것도 하지 않으셨다면, 고객님의 Elcap Firewall 정책은 INPUT, OUTPUT 허용입니다. 즉 방화벽에서 고객님서버의 패킷은 무조건 허용입니다.



Elcap Firewall을 사용 하시려면,
가장 먼저 할 사항은 Elcap Firewall 초기화를 하여야 합니다.
Elcap Firewall 초기화를 하지 않고는 다른 서비스를 받을 수 없습니다.

Q-8) Elcap Firewall 초기화는 어떻게 하는 건가요?

A-8) 1. Elcap 초기화를 선택합니다. **[#그림 3.1]**

2. 확인버튼을 선택하시면, 고객님의 서버를 PORTSCAN을 시작합니다. **[#그림 3.2]**

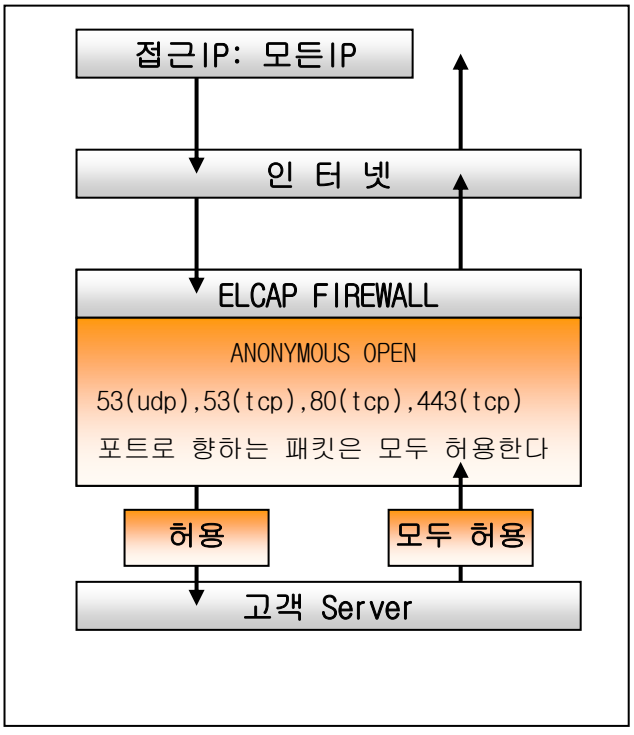
3. PORTSCAN 한 결과를 Elcap 정책으로 변형을 한 후 정책에 반영을 합니다.
[#그림 3.3] ~ [#그림 3.4]

4. 세부설명

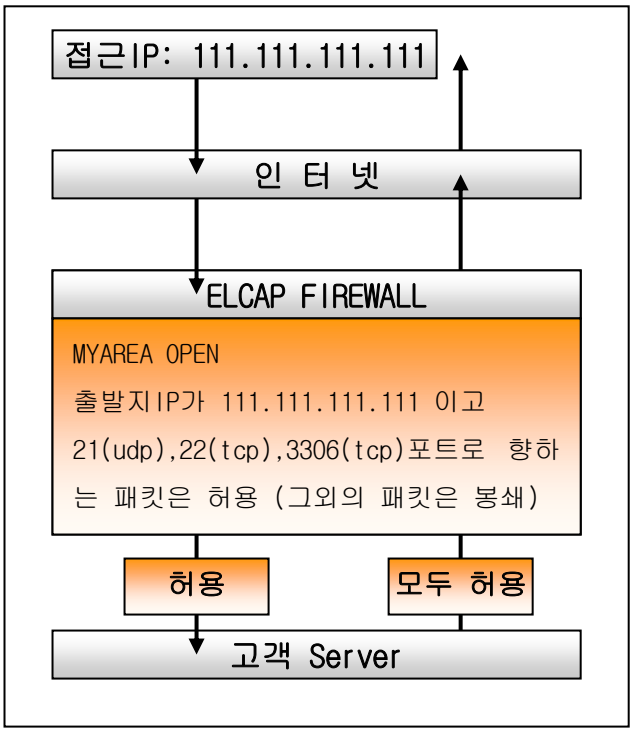
고객님의 서버를 PortScan 한 후 Elcap Firewall 정책으로 변경을 합니다.

예를 들어 **ANONYMOUS OPEN** 은 53(udp), 53(tcp), 80(tcp), 443(tcp) 를 선택 or 등록
MYAREA OPEN 은 21(tcp), 22(tcp), 3306(tcp)을 선택 or 등록
접근가능 IP 는 111.111.111.111 으로 선택 or 변경
MANAGE IP 는 222.222.222.222 으로 선택 or 변경,
특정서버접근 는 22(tcp), 25(tcp), http(80) 을 선택 or 등록 하셨다면,
Elcap Firewall 정책에 따라 패킷은
아래의 그림과 같이 동작하게 됩니다.

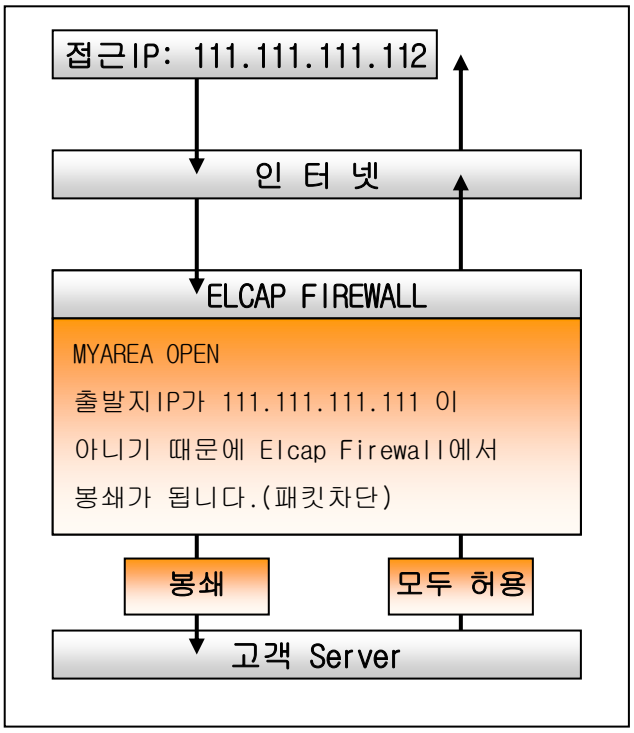
ANONYMOUS OPEN 그림 설명



MYAREA OPEN 그림 설명(1)



MYAREA OPEN 그림 설명(2)

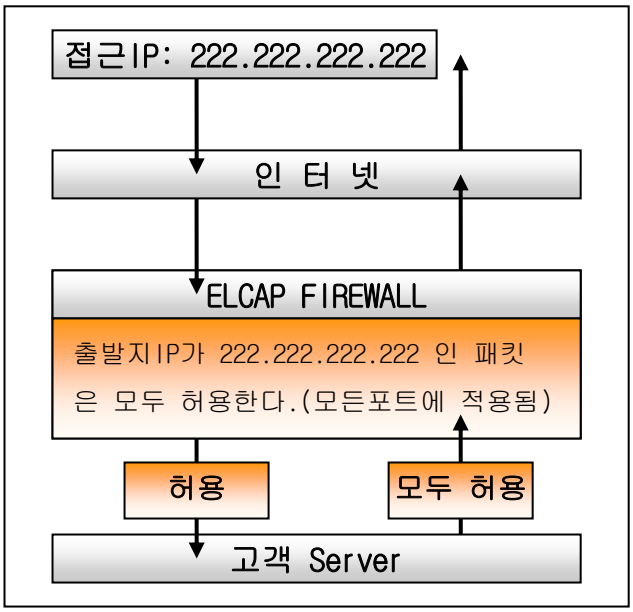


ANONYMOUS OPEN - 접근IP가 어떤 것이든 상관없이 등록된 포트로 들어오는 패킷을 모두 허용합니다.

MYAREA OPEN - 등록된IP or 등록된 IP대역 에서만 등록된 포트로 들어오는 패킷만을 허용합니다.
(IP를 등록할 때 대역으로 입력이 가능합니다. APPEND A를 참고 하십시오)

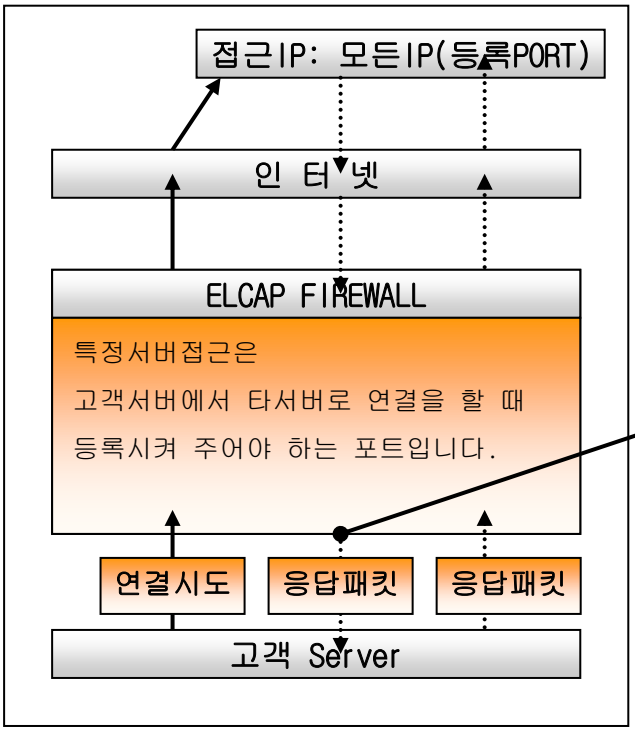
등록되지 않은 포트는 모두 봉쇄입니다.

MANAGE IP 그림 설명



MANAGE IP – MANAGE IP 로 등록된 IP는 ANONYMOUS, MYAREA, ALWAYS 정책에 관계없이
모든 접근을 허용합니다.

특정서버접근 그림 설명



특정서버접근 포트를 등록시켜 주지
않았다면 응답패킷을 받을 때
Elcap Firewall에서 패킷을
봉쇄 시키므로 연결을 설정할 수 없음.

주의) 특정서버접근은 ANONYMOUS OPEN, MYAREA OPEN, MANAGE IP 와 다른 정책입니다.
특정서버접근은 고객서버에서 다른서버로 접근할 경우의 정책입니다.
즉 고객서버에서 타서버로 접근을 하신다면,
타서버 접근포트를 등록시켜 주어야 접근이 가능합니다.

특정서버접근의 기술적인 설명(TCP 프로토콜일 경우)
TCP 프로토콜은 3번의 패킷을(three-way handshake) 주고 받은 후에야 TCP 연결을 완료 합니다. 데이터 전송도 마찬가지 입니다.
만약 Elcap Firewall 정책에서 항상 OUTPUT은 허용되지만, 2번째 패킷(상대방 서버에서 고객서버로 들어오는 응답 패킷)은 Elcap Firewall에 봉쇄되어 연결이 설정이 되지 않습니다.
그렇기 때문에 Elcap Firewall에서 Source Port
(Web을 사용한다면 80번 포트를, SSH를 사용한다면 22 포트를) 등록시켜 주는 것입니다.

Q-9) Elcap Firewall을 초기화를 했습니다. 그래서 Elcap 정책이 적용이 되는 것 같은데, Elcap Firewall을 사용하기 너무 복잡하고 어렵습니다. 그래서 Elcap Firewall 사용을 안 할려고 합니다. 어떻게 해야 하나요?

A-9) 타 방화벽에 비해 Elcap Firewall은 고객님이 이해하기 쉽게 만들어졌습니다.
매뉴얼을 한번 더 살펴보시고 Elcap Firewall을 사용하시는 것이 고객님을 위해서 더 좋을 것입니다.
방화벽을 사용하지 않는다면, 고객님 서버는 해커들의 표적이 될 것입니다. 또한 고객님의 귀중한 자료도 안전하다고 보장해 드릴 수는 없습니다. Elcap Firewall을 사용하신다면, 적어도 90% 이상의 불법적인 접근은 막을 수 있습니다.
그래도 Elcap Firewall을 사용하지 않으실 거라면,
Elcap 해제 => 확인을 누르시면, 고객님의 서버로 향하는 패킷은 Elcap Firewall에서 필터링 되지 않을 것입니다.

Q-10) 저희는 유동IP를 이용하여 인터넷을 사용하는 회사입니다.
가끔식 IP가 바뀌는 문제가 있는데, 이런 경우에도 Elcap Firewall을 사용할 수 있습니까?

A-10) 문제는 되지 않습니다.
두가지 방법이 있습니다.

첫번째 방법은
가장 올바른 방법이지만, IP를 변경 되었을 때마다 서버관리자가 매번 접속하여
MY AREA OPEN에 등록된 IP를 변경된 IP로 갱신하여 주는 방법입니다.

두번째 방법은
서버관리자의 번거로운 작업이 많이 줄일 수 있는 방법입니다.
단 유동 IP는 비교적 같은 대역 내에서 변경 되는 경우가 있으므로 아예 해당 대역을
등록하여 사용 하시면 관리에 편합니다.
다시말해 사무실의 유동 IP가 58.56.12.3 으로 잡혀있다면, 변경이 되더라도
58.56.12.1 ~ 255 사이의 IP내에[서 변경 되는 특징을 가집니다.
따라서 MYAREA OPEN 과 MANAGE IP에 등록할 때 IP를 대역으로
등록하여 주시면, 유동IP가 해당 대역에서 변경이 되더라도 접속이 끊기거나,
서버관리자의 번거로운 작업은 없이 질 것입니다.
즉 MYAREA OPEN 과 MANAGE IP에 58.56.12.0/24로 입력하여 주시면 58.56.12.1 ~ 255
사이에 유동IP가 잡히더라도 일일이 MYAREA OPEN, MANAGE IP의 IP를 변경하여
주지 않아도 됩니다. (대역으로 등록 하는 방법은 APPEND A를 참고 하십시오)

조금은 번거롭더라도 저는 첫번째 방법을 권해 드립니다.

Q-11) 저희는 유동IP에 공유기를 연결하여 여러 명이 인터넷을 사용하고
있습니다. 이 경우에도 Elcap Firewall을 사용하는데 문제가 없습니까?

A-11) 문제는 되지 않습니다.
아시겠지만, 사설IP를 사용하시더라도, 실제적으로 외부로 나가는 IP는 하나의 IP 입니다.
그러니, 외부로 나가는 IP를 MYAREA OPEN 과 MANAGE IP에 등록하여 주시면
Elcap Firewall 사용하시는 데 문제가 없습니다. 유동IP가 변경되는 문제는
위의 질문의 답변을 참고하시기 바랍니다.

Q-12) 두 회사가 프로젝트를 협업하여 진행하고 있습니다.
Elcap Firewall에서 어떻게 설정하는 것이 가장 효율적일까요?

A-12) 프로젝트의 특성에 따라 정책설정이 바뀔 수 있습니다.
일반적인 방법은 프로젝트의 메인을 잡은 회사의 IP를 MANAGE IP로 등록을 시켜 주시고,
MYAREA OPEN 정책에 프로젝트를 진행하는 두 회사의 IP or IP대역으로 입력하여 주시면,
네트워크를 통해서 작업하시는 협업 작업은 문제가 없을 듯 합니다.

9. APPEND A (IP를 대역으로 등록 할 경우의 사용 예)

1. Elcap Firewall은 IP 대역을 지원하기 위해 입력되는 IP는 모두 IP대역으로도 입력할 수 있게 제작되었습니다.
   고객님들이 입력하고 싶어하시는 IP 대역을 [입력하고 싶은 IP 범위] 찾으시고,
   찾으신 대역 옆에 있는 [IP 대역으로 변환] 숫치를 입력하여 주시면 됩니다.

몇 개의 예를 들어 설명하겠습니다.
첫번째 예) MYAREA OPEN 정책에 목적지 포트를 22번으로 접근주소를
201.148.12.1 ~ 50까지 입력하고 싶으시다면, 아래의 표를 참고하시면,

=> 아래와 같이 입력하시면 됩니다.
201.148.12.1 ~ 31까지의 대역 : 201.148.12.0/27
201.148.12.32 ~ 47까지의 대역 : 201.148.12.32/28
201.148.12.48 ~ 49까지의 대역 : 201.148.12.48/31
201.148.12.50
이렇게 4번 입력하여 주시면, 1 ~ 50번까지 대역을 입력한 것입니다.

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.1 ~ 31	210.118.169.0/27	31개의 IP 대역
210.118.169.32 ~ 63	210.118.169.32/27	32개의 IP 대역
…	…	…
210.118.169.32 ~ 47	210.118.169.32/28	16개의 IP 대역
210.118.169.48 ~ 63	210.118.169.48/28	16개의 IP 대역
…	…	…
210.118.169.48 ~ 49	210.118.169.48/31	2개의 IP 대역
210.118.169.50 ~ 51	210.118.169.50/31	2개의 IP 대역

=> IP가 추가될 가능성이 있다면
201.148.12.1 ~ 63까지의 대역 : 201.148.12.0/26

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.1 ~ 63	210.118.169.0/26	63개의 IP 대역
210.118.169.64 ~ 127	210.118.169.64/26	64개의 IP 대역
…	…	…

두번째 예) 고객님께서 유동IP 59.11.77.111를 사용하시는 중이라고 가정을 한다면,
고객님께서 25번 포트를 해당 IP에서만 허용시키고자 한다면,
MYAREA OPEN 정책에 해당 IP를 입력시켜 준다면, 추후 IP변동이 있을 경우 모든 포트에 대해서 바뀐 IP로 갱신시켜야 한다.
만약 대역으로 입력하신다면, 유동IP가 변하는 대역 59.11.77.0 ~ 255 를 등록하여 주시면, 유동IP가 59.11.77.1~255 대역에서 바뀐다고 하더라도, 고객님께서 접근하실 때 전혀 문제가 되지 않습니다.

=> 59.11.77.1 ~ 255 까지의 대역 : 59.11.77.0/24
로 입력하여 주시면 됩니다.

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.1 ~ 255	210.118.169.0/24	255개의 IP 대역

2. IP를 대역 계산방법

아래의 표는 일반 방화벽 대역을 계산하는 방법입니다.
복잡하시다고 한다면, 굳이 읽지 않으셔도 아래의 표만 참고하신다면, IP 대역입력에 전혀 문제가 되지 않습니다.
그렇지만, 계산방법을 한번 살펴보시면, 다른 곳에 활용을 하실 수 있으실 겁니다.

대역 계산에 앞서 IP가 어떻게 계산되는지 보도록하겠습니다.

IP의 각각의 숫자는 비트로 구성되어 있습니다.
IP가 210.118.169.54 이라면,

각각의 숫자는 아래와 같이 비트로 구성되어 있습니다.
숫자 210는 각 비트가 1 1 0 1 0 0 1 0 각 비트가
(2의7승) + (2의6승) + (2의4승) + (2의1승) 는 128 + 64 + 16 + 2 은 210 입니다.
숫자 118는 각 비트가 0 1 1 1 0 1 1 0 각 비트가
(2의6승) + (2의5승) + (2의4승) + (2의2승) + (2의1승) 는 64 + 32 + 16 + 4 + 2 은 118 입니다.
숫자 169는 각 비트가 1 0 1 0 1 0 0 1 각 비트가
(2의7승) + (2의5승) + (2의3승) + (2의0승) 는 128 + 32 + 8 + 1 은 169 입니다.
숫자 54는 각 비트가 0 0 1 1 0 1 1 0 각 비트가
(2의5승) + (2의4승) + (2의2승) + (2의1승) 는 32 + 16 + 4 + 2 은 54 입니다.

아래의 그림처럼 구성이 됩니다.

0	1	2	3	4	5	6	7	.	8	9	10	11	12	13	14	15	.	16	17	18	19	20	21	22	23	.	24	25	26	27	28	29	30	31
1	1	0	1	0	0	1	0	.	0	1	1	1	0	1	1	0	.	1	0	1	0	1	0	0	1	.	0	0	1	1	0	1	1	0

그럼 IP대역을 계산하는 방법을 몇가지 예로 보도록 하겠습니다.

0/24의 의미

0의 의미는 맨 마지막 IP의 숫자가 0부터 시작한다는 의미입니다.
/의 의미는 ~ 로 생각하시면 됩니다.
가장 중요한 24의 의미는 24bit에서 31bit 까지 1이라는 의미입니다.
(2의 7승) + (2의 6승) + (2의 5승) + (2의 4승) + (2의 3승) + (2의 2승) +
(2의 1승) + (2의 0승) 을 더하면 255 입니다. (255개의 IP 개수를 의미합니다.)
0부터 시작하여 (0 + 255) 까지가 됩니다.

0	1	2	3	4	5	6	7	.	8	9	10	11	12	13	14	15	.	16	17	18	19	20	21	22	23	.	24	25	26	27	28	29	30	31
1	1	0	1	0	0	1	0	.	0	1	1	1	0	1	1	0	.	1	0	1	0	1	0	0	1	.	1	1	1	1	1	1	1	1

0/25의 의미

0의 의미는 맨 마지막 IP의 숫자가 0부터 시작한다는 의미입니다.
/의 의미는 ~ 로 생각하시면 됩니다.
가장 중요한 25의 의미는 25bit에서 31bit 까지 1이라는 의미입니다.
(2의 6승) + (2의 5승) + (2의 4승) + (2의 3승) + (2의 2승) + (2의 1승) +
(2의 0승) 을 더하면 127 입니다. (127개의 IP 개수를 의미합니다.)
0부터 (0+127)까지 라는 의미입니다.

128/25의 의미

128의 의미는 맨 마지막 IP의 숫자가 128부터 시작한다는 의미입니다.
/의 의미는 ~ 로 생각하시면 됩니다.
가장 중요한 25의 의미는 25bit에서 31bit 까지 1이라는 의미입니다.
(2의 6승) + (2의 5승) + (2의 4승) + (2의 3승) + (2의 2승) + (2의 1승) +
(2의 0승) 을 더하면 127 입니다.
128부터 (128 + 127 = 255) 까지 라는 의미입니다.

0	1	2	3	4	5	6	7	.	8	9	10	11	12	13	14	15	.	16	17	18	19	20	21	22	23	.	24	25	26	27	28	29	30	31
1	1	0	1	0	0	1	0	.	0	1	1	1	0	1	1	0	.	1	0	1	0	1	0	0	1	.	0	1	1	1	1	1	1	1

위의 계산처럼, 아래의 표의 대역을 한번 계산해 보십시오.

[210.118.169.1~255 범위로 예를들어 IP 대역으로 변환]

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.1 ~ 255	210.118.169.0/24	255개의 IP 대역
210.118.169.1 ~ 127	210.118.169.0/25	127개의 IP 대역
210.118.169.128 ~ 255	210.118.169.128/25	128개의 IP 대역
210.118.169.1 ~ 63	210.118.169.0/26	63개의 IP 대역
210.118.169.64 ~ 127	210.118.169.64/26	64개의 IP 대역
210.118.169.128 ~ 191	210.118.169.128/26	64개의 IP 대역
210.118.169.192 ~ 255	210.118.169.192/26	64개의 IP 대역
210.118.169.1 ~ 31	210.118.169.0/27	31개의 IP 대역
210.118.169.32 ~ 63	210.118.169.32/27	32개의 IP 대역
210.118.169.64 ~ 95	210.118.169.64/27	32개의 IP 대역
210.118.169.96 ~ 127	210.118.169.96/27	32개의 IP 대역
210.118.169.128 ~ 159	210.118.169.128/27	32개의 IP 대역
210.118.169.160 ~ 191	210.118.169.160/27	32개의 IP 대역
210.118.169.192 ~ 223	210.118.169.192/27	32개의 IP 대역
210.118.169.224 ~ 255	210.118.169.224/27	32개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.1 ~ 255	210.118.169.0/24	255개의 IP 대역
210.118.169.1 ~ 127	210.118.169.0/25	127개의 IP 대역
210.118.169.128 ~ 255	210.118.169.128/25	128개의 IP 대역
210.118.169.1 ~ 63	210.118.169.0/26	63개의 IP 대역
210.118.169.64 ~ 127	210.118.169.64/26	64개의 IP 대역
210.118.169.128 ~ 191	210.118.169.128/26	64개의 IP 대역
210.118.169.192 ~ 255	210.118.169.192/26	64개의 IP 대역
210.118.169.1 ~ 31	210.118.169.0/27	31개의 IP 대역
210.118.169.32 ~ 63	210.118.169.32/27	32개의 IP 대역
210.118.169.64 ~ 95	210.118.169.64/27	32개의 IP 대역
210.118.169.96 ~ 127	210.118.169.96/27	32개의 IP 대역
210.118.169.128 ~ 159	210.118.169.128/27	32개의 IP 대역
210.118.169.160 ~ 191	210.118.169.160/27	32개의 IP 대역
210.118.169.192 ~ 223	210.118.169.192/27	32개의 IP 대역
210.118.169.224 ~ 255	210.118.169.224/27	32개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.1 ~ 15	210.118.169.0/28	15개의 IP 대역
210.118.169.16 ~ 31	210.118.169.16/28	16개의 IP 대역
210.118.169.32 ~ 47	210.118.169.32/28	16개의 IP 대역
210.118.169.48 ~ 63	210.118.169.48/28	16개의 IP 대역
210.118.169.64 ~ 79	210.118.169.64/28	16개의 IP 대역
210.118.169.80 ~ 95	210.118.169.80/28	16개의 IP 대역
210.118.169.96 ~ 111	210.118.169.96/28	16개의 IP 대역
210.118.169.112 ~ 127	210.118.169.112/28	16개의 IP 대역
210.118.169.128 ~ 143	210.118.169.128/28	16개의 IP 대역
210.118.169.144 ~ 159	210.118.169.144/28	16개의 IP 대역
210.118.169.160 ~ 175	210.118.169.160/28	16개의 IP 대역
210.118.169.176 ~ 191	210.118.169.176/28	16개의 IP 대역
210.118.169.192 ~ 207	210.118.169.192/28	16개의 IP 대역
210.118.169.208 ~ 223	210.118.169.208/28	16개의 IP 대역
210.118.169.224 ~ 239	210.118.169.224/28	16개의 IP 대역
210.118.169.240 ~ 255	210.118.169.240/28	16개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.1 ~ 7	210.118.169.0/29	7개의 IP 대역
210.118.169.8 ~ 15	210.118.169.8/29	8개의 IP 대역
210.118.169.16 ~ 23	210.118.169.16/29	8개의 IP 대역
210.118.169.24 ~ 31	210.118.169.24/29	8개의 IP 대역
210.118.169.32 ~ 39	210.118.169.32/29	8개의 IP 대역
210.118.169.40 ~ 47	210.118.169.40/29	8개의 IP 대역
210.118.169.48 ~ 55	210.118.169.48/29	8개의 IP 대역
210.118.169.56 ~ 63	210.118.169.56/29	8개의 IP 대역
210.118.169.64 ~ 71	210.118.169.64/29	8개의 IP 대역
210.118.169.72 ~ 79	210.118.169.72/29	8개의 IP 대역
210.118.169.80 ~ 87	210.118.169.80/29	8개의 IP 대역
210.118.169.88 ~ 95	210.118.169.88/29	8개의 IP 대역
210.118.169.96 ~ 103	210.118.169.96/29	8개의 IP 대역
210.118.169.104 ~ 111	210.118.169.104/29	8개의 IP 대역
210.118.169.112 ~ 119	210.118.169.112/29	8개의 IP 대역
210.118.169.120 ~ 127	210.118.169.120/29	8개의 IP 대역
210.118.169.128 ~ 135	210.118.169.128/29	8개의 IP 대역
210.118.169.136 ~ 143	210.118.169.136/29	8개의 IP 대역
210.118.169.144 ~ 151	210.118.169.144/29	8개의 IP 대역
210.118.169.152 ~ 159	210.118.169.152/29	8개의 IP 대역
210.118.169.160 ~ 167	210.118.169.160/29	8개의 IP 대역
210.118.169.168 ~ 175	210.118.169.168/29	8개의 IP 대역
210.118.169.176 ~ 183	210.118.169.176/29	8개의 IP 대역
210.118.169.184 ~ 191	210.118.169.184/29	8개의 IP 대역
210.118.169.192 ~ 199	210.118.169.192/29	8개의 IP 대역
210.118.169.200 ~ 207	210.118.169.200/29	8개의 IP 대역
210.118.169.208 ~ 215	210.118.169.208/29	8개의 IP 대역
210.118.169.216 ~ 223	210.118.169.216/29	8개의 IP 대역
210.118.169.224 ~ 231	210.118.169.224/29	8개의 IP 대역
210.118.169.232 ~ 239	210.118.169.232/29	8개의 IP 대역
210.118.169.240 ~ 247	210.118.169.240/29	8개의 IP 대역
210.118.169.248 ~ 255	210.118.169.248/29	8개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.1 ~ 3	210.118.169.0/30	3개의 IP 대역
210.118.169.4 ~ 7	210.118.169.4/30	4개의 IP 대역
210.118.169.8 ~ 11	210.118.169.8/30	4개의 IP 대역
210.118.169.12 ~ 15	210.118.169.12/30	4개의 IP 대역
210.118.169.16 ~ 19	210.118.169.16/30	4개의 IP 대역
210.118.169.20 ~ 23	210.118.169.20/30	4개의 IP 대역
210.118.169.24 ~ 27	210.118.169.24/30	4개의 IP 대역
210.118.169.28 ~ 31	210.118.169.28/30	4개의 IP 대역
210.118.169.32 ~ 35	210.118.169.32/30	4개의 IP 대역
210.118.169.36 ~ 39	210.118.169.36/30	4개의 IP 대역
210.118.169.40 ~ 43	210.118.169.40/30	4개의 IP 대역
210.118.169.44 ~ 47	210.118.169.44/30	4개의 IP 대역
210.118.169.48 ~ 51	210.118.169.48/30	4개의 IP 대역
210.118.169.52 ~ 55	210.118.169.52/30	4개의 IP 대역
210.118.169.56 ~ 59	210.118.169.56/30	4개의 IP 대역
210.118.169.60 ~ 63	210.118.169.60/30	4개의 IP 대역
210.118.169.64 ~ 67	210.118.169.64/30	4개의 IP 대역
210.118.169.68 ~ 71	210.118.169.68/30	4개의 IP 대역
210.118.169.72 ~ 75	210.118.169.72/30	4개의 IP 대역
210.118.169.76 ~ 79	210.118.169.76/30	4개의 IP 대역
210.118.169.80 ~ 83	210.118.169.80/30	4개의 IP 대역
210.118.169.84 ~ 87	210.118.169.84/30	4개의 IP 대역
210.118.169.88 ~ 91	210.118.169.88/30	4개의 IP 대역
210.118.169.92 ~ 95	210.118.169.92/30	4개의 IP 대역
210.118.169.96 ~ 99	210.118.169.96/30	4개의 IP 대역
210.118.169.100 ~ 103	210.118.169.100/30	4개의 IP 대역
210.118.169.104 ~ 107	210.118.169.104/30	4개의 IP 대역
210.118.169.108 ~ 111	210.118.169.108/30	4개의 IP 대역
210.118.169.112 ~ 115	210.118.169.112/30	4개의 IP 대역
210.118.169.116 ~ 119	210.118.169.116/30	4개의 IP 대역
210.118.169.120 ~ 123	210.118.169.120/30	4개의 IP 대역
210.118.169.124 ~ 127	210.118.169.124/30	4개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.128 ~ 131	210.118.169.128/30	4개의 IP 대역
210.118.169.132 ~ 135	210.118.169.132/30	4개의 IP 대역
210.118.169.136 ~ 139	210.118.169.136/30	4개의 IP 대역
210.118.169.140 ~ 143	210.118.169.140/30	4개의 IP 대역
210.118.169.144 ~ 147	210.118.169.144/30	4개의 IP 대역
210.118.169.148 ~ 151	210.118.169.148/30	4개의 IP 대역
210.118.169.152 ~ 155	210.118.169.152/30	4개의 IP 대역
210.118.169.156 ~ 159	210.118.169.156/30	4개의 IP 대역
210.118.169.160 ~ 163	210.118.169.160/30	4개의 IP 대역
210.118.169.164 ~ 167	210.118.169.164/30	4개의 IP 대역
210.118.169.168 ~ 171	210.118.169.168/30	4개의 IP 대역
210.118.169.172 ~ 175	210.118.169.172/30	4개의 IP 대역
210.118.169.176 ~ 179	210.118.169.176/30	4개의 IP 대역
210.118.169.180 ~ 183	210.118.169.180/30	4개의 IP 대역
210.118.169.184 ~ 187	210.118.169.184/30	4개의 IP 대역
210.118.169.188 ~ 191	210.118.169.188/30	4개의 IP 대역
210.118.169.192 ~ 195	210.118.169.192/30	4개의 IP 대역
210.118.169.196 ~ 199	210.118.169.196/30	4개의 IP 대역
210.118.169.200 ~ 203	210.118.169.200/30	4개의 IP 대역
210.118.169.204 ~ 207	210.118.169.204/30	4개의 IP 대역
210.118.169.208 ~ 211	210.118.169.208/30	4개의 IP 대역
210.118.169.212 ~ 215	210.118.169.212/30	4개의 IP 대역
210.118.169.216 ~ 219	210.118.169.216/30	4개의 IP 대역
210.118.169.220 ~ 223	210.118.169.220/30	4개의 IP 대역
210.118.169.224 ~ 227	210.118.169.224/30	4개의 IP 대역
210.118.169.228 ~ 231	210.118.169.228/30	4개의 IP 대역
210.118.169.232 ~ 235	210.118.169.232/30	4개의 IP 대역
210.118.169.236 ~ 239	210.118.169.236/30	4개의 IP 대역
210.118.169.240 ~ 243	210.118.169.240/30	4개의 IP 대역
210.118.169.244 ~ 247	210.118.169.244/30	4개의 IP 대역
210.118.169.248 ~ 251	210.118.169.248/30	4개의 IP 대역
210.118.169.252 ~ 255	210.118.169.252/30	4개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.2 ~ 3	210.118.169.2/31	2개의 IP 대역
210.118.169.4 ~ 5	210.118.169.4/31	2개의 IP 대역
210.118.169.6 ~ 7	210.118.169.6/31	2개의 IP 대역
210.118.169.8 ~ 9	210.118.169.8/31	2개의 IP 대역
210.118.169.10 ~ 11	210.118.169.10/31	2개의 IP 대역
210.118.169.12 ~ 13	210.118.169.12/31	2개의 IP 대역
210.118.169.14 ~ 15	210.118.169.14/31	2개의 IP 대역
210.118.169.16 ~ 17	210.118.169.16/31	2개의 IP 대역
210.118.169.18 ~ 19	210.118.169.18/31	2개의 IP 대역
210.118.169.20 ~ 21	210.118.169.20/31	2개의 IP 대역
210.118.169.22 ~ 23	210.118.169.22/31	2개의 IP 대역
210.118.169.24 ~ 25	210.118.169.24/31	2개의 IP 대역
210.118.169.26 ~ 27	210.118.169.26/31	2개의 IP 대역
210.118.169.28 ~ 29	210.118.169.28/31	2개의 IP 대역
210.118.169.30 ~ 31	210.118.169.30/31	2개의 IP 대역
210.118.169.32 ~ 33	210.118.169.32/31	2개의 IP 대역
210.118.169.34 ~ 35	210.118.169.34/31	2개의 IP 대역
210.118.169.36 ~ 37	210.118.169.36/31	2개의 IP 대역
210.118.169.38 ~ 39	210.118.169.38/31	2개의 IP 대역
210.118.169.40 ~ 41	210.118.169.40/31	2개의 IP 대역
210.118.169.42 ~ 43	210.118.169.42/31	2개의 IP 대역
210.118.169.44 ~ 45	210.118.169.44/31	2개의 IP 대역
210.118.169.46 ~ 47	210.118.169.46/31	2개의 IP 대역
210.118.169.48 ~ 49	210.118.169.48/31	2개의 IP 대역
210.118.169.50 ~ 51	210.118.169.50/31	2개의 IP 대역
210.118.169.52 ~ 53	210.118.169.52/31	2개의 IP 대역
210.118.169.54 ~ 55	210.118.169.54/31	2개의 IP 대역
210.118.169.56 ~ 57	210.118.169.56/31	2개의 IP 대역
210.118.169.58 ~ 59	210.118.169.58/31	2개의 IP 대역
210.118.169.60 ~ 61	210.118.169.60/31	2개의 IP 대역
210.118.169.62 ~ 63	210.118.169.62/31	2개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.64 ~ 65	210.118.169.64/31	2개의 IP 대역
210.118.169.66 ~ 67	210.118.169.66/31	2개의 IP 대역
210.118.169.68 ~ 69	210.118.169.68/31	2개의 IP 대역
210.118.169.70 ~ 71	210.118.169.70/31	2개의 IP 대역
210.118.169.72 ~ 73	210.118.169.72/31	2개의 IP 대역
210.118.169.74 ~ 75	210.118.169.74/31	2개의 IP 대역
210.118.169.76 ~ 77	210.118.169.76/31	2개의 IP 대역
210.118.169.78 ~ 79	210.118.169.78/31	2개의 IP 대역
210.118.169.80 ~ 81	210.118.169.80/31	2개의 IP 대역
210.118.169.82 ~ 83	210.118.169.82/31	2개의 IP 대역
210.118.169.84 ~ 85	210.118.169.84/31	2개의 IP 대역
210.118.169.86 ~ 87	210.118.169.86/31	2개의 IP 대역
210.118.169.88 ~ 89	210.118.169.88/31	2개의 IP 대역
210.118.169.90 ~ 91	210.118.169.90/31	2개의 IP 대역
210.118.169.92 ~ 93	210.118.169.92/31	2개의 IP 대역
210.118.169.94 ~ 95	210.118.169.94/31	2개의 IP 대역
210.118.169.96 ~ 97	210.118.169.96/31	2개의 IP 대역
210.118.169.98 ~ 99	210.118.169.98/31	2개의 IP 대역
210.118.169.100 ~ 101	210.118.169.100/31	2개의 IP 대역
210.118.169.102 ~ 103	210.118.169.102/31	2개의 IP 대역
210.118.169.104 ~ 105	210.118.169.104/31	2개의 IP 대역
210.118.169.106 ~ 107	210.118.169.106/31	2개의 IP 대역
210.118.169.108 ~ 109	210.118.169.108/31	2개의 IP 대역
210.118.169.110 ~ 111	210.118.169.110/31	2개의 IP 대역
210.118.169.112 ~ 113	210.118.169.112/31	2개의 IP 대역
210.118.169.114 ~ 115	210.118.169.114/31	2개의 IP 대역
210.118.169.116 ~ 117	210.118.169.116/31	2개의 IP 대역
210.118.169.118 ~ 119	210.118.169.118/31	2개의 IP 대역
210.118.169.120 ~ 121	210.118.169.120/31	2개의 IP 대역
210.118.169.122 ~ 123	210.118.169.122/31	2개의 IP 대역
210.118.169.124 ~ 125	210.118.169.124/31	2개의 IP 대역
210.118.169.126 ~ 127	210.118.169.126/31	2개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.128 ~ 129	210.118.169.128/31	2개의 IP 대역
210.118.169.130 ~ 131	210.118.169.130/31	2개의 IP 대역
210.118.169.132 ~ 133	210.118.169.132/31	2개의 IP 대역
210.118.169.134 ~ 135	210.118.169.134/31	2개의 IP 대역
210.118.169.136 ~ 137	210.118.169.136/31	2개의 IP 대역
210.118.169.138 ~ 139	210.118.169.138/31	2개의 IP 대역
210.118.169.140 ~ 141	210.118.169.140/31	2개의 IP 대역
210.118.169.142 ~ 143	210.118.169.142/31	2개의 IP 대역
210.118.169.144 ~ 145	210.118.169.144/31	2개의 IP 대역
210.118.169.146 ~ 147	210.118.169.146/31	2개의 IP 대역
210.118.169.148 ~ 149	210.118.169.148/31	2개의 IP 대역
210.118.169.150 ~ 151	210.118.169.150/31	2개의 IP 대역
210.118.169.152 ~ 153	210.118.169.152/31	2개의 IP 대역
210.118.169.154 ~ 155	210.118.169.154/31	2개의 IP 대역
210.118.169.156 ~ 157	210.118.169.156/31	2개의 IP 대역
210.118.169.158 ~ 159	210.118.169.158/31	2개의 IP 대역
210.118.169.160 ~ 161	210.118.169.160/31	2개의 IP 대역
210.118.169.162 ~ 163	210.118.169.162/31	2개의 IP 대역
210.118.169.164 ~ 165	210.118.169.164/31	2개의 IP 대역
210.118.169.166 ~ 167	210.118.169.166/31	2개의 IP 대역
210.118.169.168 ~ 169	210.118.169.168/31	2개의 IP 대역
210.118.169.170 ~ 171	210.118.169.170/31	2개의 IP 대역
210.118.169.172 ~ 173	210.118.169.172/31	2개의 IP 대역
210.118.169.174 ~ 175	210.118.169.174/31	2개의 IP 대역
210.118.169.176 ~ 177	210.118.169.176/31	2개의 IP 대역
210.118.169.178 ~ 179	210.118.169.178/31	2개의 IP 대역
210.118.169.180 ~ 181	210.118.169.180/31	2개의 IP 대역
210.118.169.182 ~ 183	210.118.169.182/31	2개의 IP 대역
210.118.169.184 ~ 185	210.118.169.184/31	2개의 IP 대역
210.118.169.186 ~ 187	210.118.169.186/31	2개의 IP 대역
210.118.169.188 ~ 189	210.118.169.188/31	2개의 IP 대역
210.118.169.190 ~ 191	210.118.169.190/31	2개의 IP 대역

입력하고 싶은 IP 범위	IP 대역으로 변환	비고
210.118.169.192 ~ 193	210.118.169.192/31	2개의 IP 대역
210.118.169.194 ~ 195	210.118.169.194/31	2개의 IP 대역
210.118.169.196 ~ 197	210.118.169.196/31	2개의 IP 대역
210.118.169.198 ~ 199	210.118.169.198/31	2개의 IP 대역
210.118.169.200 ~ 201	210.118.169.200/31	2개의 IP 대역
210.118.169.202 ~ 203	210.118.169.202/31	2개의 IP 대역
210.118.169.204 ~ 205	210.118.169.204/31	2개의 IP 대역
210.118.169.206 ~ 207	210.118.169.206/31	2개의 IP 대역
210.118.169.208 ~ 209	210.118.169.208/31	2개의 IP 대역
210.118.169.210 ~ 211	210.118.169.210/31	2개의 IP 대역
210.118.169.212 ~ 213	210.118.169.212/31	2개의 IP 대역
210.118.169.214 ~ 215	210.118.169.214/31	2개의 IP 대역
210.118.169.216 ~ 217	210.118.169.216/31	2개의 IP 대역
210.118.169.218 ~ 219	210.118.169.218/31	2개의 IP 대역
210.118.169.220 ~ 221	210.118.169.220/31	2개의 IP 대역
210.118.169.222 ~ 223	210.118.169.222/31	2개의 IP 대역
210.118.169.224 ~ 225	210.118.169.224/31	2개의 IP 대역
210.118.169.226 ~ 227	210.118.169.226/31	2개의 IP 대역
210.118.169.228 ~ 229	210.118.169.228/31	2개의 IP 대역
210.118.169.230 ~ 231	210.118.169.230/31	2개의 IP 대역
210.118.169.232 ~ 233	210.118.169.232/31	2개의 IP 대역
210.118.169.234 ~ 235	210.118.169.234/31	2개의 IP 대역
210.118.169.236 ~ 237	210.118.169.236/31	2개의 IP 대역
210.118.169.238 ~ 239	210.118.169.238/31	2개의 IP 대역
210.118.169.240 ~ 241	210.118.169.240/31	2개의 IP 대역
210.118.169.242 ~ 243	210.118.169.242/31	2개의 IP 대역
210.118.169.244 ~ 245	210.118.169.244/31	2개의 IP 대역
210.118.169.246 ~ 247	210.118.169.246/31	2개의 IP 대역
210.118.169.248 ~ 249	210.118.169.248/31	2개의 IP 대역
210.118.169.250 ~ 251	210.118.169.250/31	2개의 IP 대역
210.118.169.252 ~ 253	210.118.169.252/31	2개의 IP 대역
210.118.169.254 ~ 255	210.118.169.254/31	2개의 IP 대역