Lars Krahl
Stand: 2006

Grundlagen PIX-Firewall

Grundkonfiguration, Sicherung, Reset, Logging

Einleitung

Dieses Dokument befasst sich mit den Grundlagen der Bedienung der Cisco PIX-Firewall. Die Aufgaben beziehen sich auf PIX Version 6.3(3) und können bei anderen Versionen variieren. Der gesamte Auftrag wird auf Terminalebene durchgeführt.

Vorbereitungen

Es ist sicherzustellen, das per Terminalanwendung (z.B. Hyperterminal) auf den Konsolenport zugegriffen werden kann. Weiterhin sollte ein funktionierender TFTP-Server bereitstehen. Ausserdem sollten grundlegende Kenntnisse zur Bedienung von Ciscos IOS vorhanden sein.

1. Allgemein

1. 1. Neben der Konfiguration per Terminal gibt es weitere Möglichkeiten, dies zu tun. Welche sind das?

Antwort:

-
-

1. 2. Stellen Sie eine Terminalverbindung mit der PIX her!

1. 3. Wechseln Sie in den privileged-Modus!

Befehl: ……

Welches Passwort ist dabei standardmässig eingestellt?

Antwort: ……

1. 4. Lassen Sie sich die Versionsinformationen anzeigen

Befehl: ……

IOS Version:
Prozessor:
RAM:
Flash:

1. 5. Lassen Sie sich die Schnittstellen anzeigen!

Befehl: ……

1. 6. Geben Sie die Namen der Schnittstellen an!

Ethernet0 –
Ethernet1 –
Ethernet2 (nur bei PIX 501) –

1. 7. Lassen Sie sich die laufende Konfiguration anzeigen!

Befehl: ……

1. 8. Welche Unterschiede fallen Ihnen beim Hilfesystem im Gegensatz zu Cisco-Routern und – Switchen auf?
Antwort:
   -
   -
   -

1. 9. Welcher Befehl zeigt detaillierte Informationen zu einem anderen Befehl?

Befehl: ……

1. 8. Wie werden die meisten Befehle des PIX-IOS negiert?

Antwort:…….....

2. Grundkonfiguration

Folgende Passwörter werden bei Bedarf auf allen Geräten verwendet:

telnet-Passwort	:	telnet
enable-Passwort	:	enable

2. 1. Wechseln Sie in den global config-Modus!

Befehl: ……

2. 2. Setzen Sie das enable-Passwort!

Befehl: ……

2. 3. Fahren Sie das inside-Interface hoch!

Befehl: ……

2. 4. Geben Sie diesem Interface eine geeignete IP-Adresse und übertragen Sie diese in den angehängten Netzplan!

Befehl: ……

2. 5. Testen Sie die Verbindung zwischen ihrem Client und dem Interface!

Befehl: ……

2. 6. Wiederholen Sie den Vorgang für das outside-Interface! Warum kann das outside-Interface noch nicht vom LAN aus erreicht werden?

Antwort:…….....

2. 7. Um im späteren Verlauf verständlichere Zugriffsregeln festzulegen, können IP-Adressen mit Bezeichnungen assoziiert werden (ähnlich DNS). Verbinden Sie Ihre IP mit einem geeigneten Namen (Bsp. PlatzX)!

Befehl: ……

2. 8. Setzen Sie das telnet-Passwort!

Befehl: ……

2. 9. Setzen Sie den Time-Out-Wert auf 60 Minuten!

Befehl: ……

2. 10. Aktivieren Sie den telnet-Zugang am inside-Interface und setzen Sie dabei den in 2.7. gesetzten Namen sinnvoll ein!

Befehl: ……

2. 11. Testen Sie den telnet-Zugang!

Befehl: ……

2. 12. Aktivieren Sie den http-basierten PDM-Server!

Befehl: ……

2. 13. Schalten Sie ihr Netz für die Benutzung des PDM am inside-Interface frei!

Befehl: ……

2. 14. Lassen Sie sich die laufende Konfiguration anzeigen!

Befehl: ……

2. 15. Speichern Sie die Einstellungen in der startup- config!

Befehl: ……

2. 16. Starten Sie einen Browser und tragen Sie in die Addressleiste ein:

https://[ip-des-inside-Interface]/

Bestätigen Sie die Sicherheitsabfragen des Browsers und loggen Sie sich mit dem enable-Passwort ein. Erscheint eine Erst-Konfigurations-Abfrage (Update Config), bestätigen Sie diese mit „Proceed“. Der PDM ist nun zum Einsatz bereit. Wechseln Sie in das Terminalprogramm zurück.

3. Reset

Auf ihrem Client ist bereits ein TFTP-Server installiert. Starten Sie ihn über die Verknüpfung „Ttftpd32“ auf dem Desktop. Er ist bereits so eingestellt, dass TFTP- und Syslog-Dienste bereitgestellt werden. Übertragene Dateien werden standardmässig im Stammverzeichnis des Programms gespeichert.

3. 1. Speichern Sie die Einstellungen auf dem TFTP- Server mit dem Namen „config“!

Befehl: ……

3. 2. Setzen Sie die Firewall zurück!

Befehl: ……

3. 3. Starten Sie die Firewall neu!

Befehl: ……

3. 4. Überspringen Sie den Konfig-Wizard und laden Sie ihre gespeicherte Konfiguration vom TFTP-Server!

Befehl: ……

4. Logging

Die Cisco PIX kann so eingerichtet werden, das Logging-Nachrichten in einem Puffer gespeichert und im Terminal ausgegeben werden. Zur genaueren Auswertung und Speicherung der Logs sollte aber ein Syslog-Server eingesetzt werden. In unserem Beispiel dient das Programm Tftpd32 als syslog daemon.

4. 1. Nennen Sie wesentliche Vorteile vom Logging!
Antwort:

-
-
-

4. 2. Nennen Sie die verschiedenen Level, die die PIX beim Logging unterscheidet!
Antwort:

0 -
1 -
2 -
3 -
4 -
5 -
6 -
7 -

4. 3. Aktivieren Sie das Logging!

Befehl: ……

4. 3. Aktivieren Sie den Zeitstempel!

Befehl: ……

4. 4. Richten Sie das Logging Level 7 auf einem Syslog-Server ein!

Befehl:…….

Befehl:…….

4. 5. Testen Sie ihre Einstellungen, indem Sie Fehlermeldungen durch Pings nach Aussen (geblockt durch fehlende Rechte) generieren!

Befehl:…….

5. Password Recovery

Das Password Recovery der PIX Firewall wird durch eine von Cisco bereitgestellte .bin-Datei realisiert. Diese löscht das eingespeicherte vergessene/mutwillig veränderte Passwort, lässt aber die Konfiguration unangetastet.

5. 1. Stellen Sie sicher, das die Datei „*np63.bin*“ im Stammverzeichnis von tftpd32 liegt. Der Dateiname leitet sich von der Version der Firewallsoftware ab. Andere Versionen lassen sich von http://www.cisco.com/warp/public/110/34.shtml#hw beziehen.

5. 2. Starten Sie tftpd32!

5. 3. ACHTUNG: Bei diesem Prozess wird die Firewall physisch neugestartet. Deshalb sollten Sie bei Bedarf ihre laufende Konfiguration in den Flash oder auf einen TFTP-Server speichern.
Ausgehend von einem Verlust des enable-Passwortes kann per Terminal nur noch der login-Bildschirm erreicht werden. Deshalb muss die PIX physisch mit dem Netzschalter aus-und eingeschaltet werden. Warten Sie innerhalb des Terminalprogramms auf die Ausgabe:

```
Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
```

Ein Druck auf ESC bringt Sie in den monitor-Modus. Lassen Sie sich die verfügbaren Befehle anzeigen!

5. 4. Setzen Sie das ethernet1 –Interface aktiv!

Befehl:…….

5. 5. Setzen Sie die IP-Adresse dieses Interfaces!

Befehl:…….

5. 6. Setzen Sie die IP des TFTP-Servers!

Befehl:…….

5. 7. Setzen Sie den *boot file name* auf *np63.bin*!

Befehl:…….

5. 8. Testen Sie die Verbindung zum TFTP-Server!

Befehl:…….

5. 9. Starten Sie den TFTP-Transfer!

Befehl:…….

5. 10. Bestätigen Sie die folgenden Abfragen und lassen Sie die PIX neu starten!

Netzplan